

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕАЛИЯХ БИЗНЕС-ТРЕБОВАНИЙ РФ

ТЕМА 2

Структура бизнес-машины

Спикер: Ануфриев Иван



ЗАНЯТИЕ 2.5

Риски ИБ в проектах цифровой трансформации.

Введение в моделирование угроз



Условное разделение информации. «Метки» на слайдах *

«Машина-времени-Time-machine» Возвращаемся и освежаем знания с прошлых занятий.	«Назад в будущее» Анонсируем то, что будет сказано на следующих занятиях	Метки по Времени
		

Рабочий «экспертный» инструментарий «Expert tools»	Примеры рабочих документов, лучшие приемы, практики и примеры использования. «Best practice»	Метки по используемым инструментам и практикам
		

Полезные мысли и выводы «Инсайты»	Соответствие требованиям, нормативная база и полезные формы по НПА	В нашем курсе, отдельно выделяется информация, относящаяся к типу «непрерывность бизнеса»	Метки по типу информации
			



Основные рассматриваемые вопросы занятия

ВОПРОС 1.1

Цифровизация
Vs
Цифровая
трансформация

ВОПРОС 1.2

Задачи бизнеса в
контексте
цифровой
трансформации

ВОПРОС 1.3

Эволюция
сервисов
безопасности

ВОПРОС 1.4

Process Mining в
контексте
цифровой
трансформации

ВОПРОС 1.5

Стандартизация
IT-процессов в
компании

1

ВОПРОС 2.1

Риски ИБ в
контексте цифровой
трансформации

ВОПРОС 2.2

Кибербезопасность
в индустрии 4.0

ВОПРОС 2.3

Проектная
статистика по
кибербезопасности
и при ЦТ

ВОПРОС 2.4

Специфика
безопасности
АСУ ТП

ВОПРОС 2.5

Введение в
моделирование
угроз по ФСТЭК

2



Основные рассматриваемые вопросы первой части занятия



ВОПРОС 1

Цифровизация
Vs
Цифровая
трансформация

ВОПРОС 2

Задачи бизнеса в
контексте
цифровой
трансформации

ВОПРОС 3

Эволюция
сервисов
безопасности

ВОПРОС 4

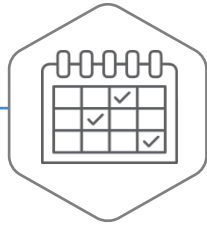
Process Mining в
контексте
цифровой
трансформации

ВОПРОС 5

Стандартизация
IT-процессов в
компании



Автоматизация, цифровизация, цифровая трансформация



АВТОМАТИЗАЦИЯ

Внедрение новых IT-
решений,
повторяющих
процессы



ЦИФРОВИЗАЦИЯ

Реинжиниринг
процессов и данные
для принятия
решения



ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

Новые модели
деятельности



Цифровизация VS цифровая трансформация



Цифровизация – улучшение существующих процессов путем внедрения информационных технологий, оптимизации и реинжиниринга, а также анализа данных для принятия решений.



Цифровая трансформация – глубокая реорганизация бизнес-процессов с широким применением цифровых инструментов для их исполнения, которая приводит к существенному (в разы) улучшению их характеристик (сокращению времени выполнения, исчезновению целых групп подпроцессов, сокращению ресурсов, затрачиваемых на выполнение процессов) и/или появлению принципиально новых их качеств и свойств.

<https://strategy.cdto.ranepa.ru/>



Цифровизация вызывает риски информационной безопасности.

Позиция отказа от использования бизнес-активностей = потеря денег

ТАРГЕТИРОВАННАЯ АТАКА



OldGremlin. MITRE ATT&CK® Mapping.

[GROUP]IB

ТАКТИКА	ТЕХНИКА	ПРОЦЕДУРА
INITIAL ACCESS	Phishing: Spearphishing Link	OldGremlin использует фишинговые ссылки на сайты, содержащие вредоносные LNK-файлы или исполняемые файлы, представляющие собой саморасширяющиеся архивы (SPX).
EXECUTION	User Execution: Malicious File Command and Scripting Interpreter: PowerShell Command and Scripting Interpreter: JavaScript/2Script	Пользователю необходимо запустить вредоносный файл, чтобы инициировать исполнение кода. OldGremlin использует обфусцированные скрипты PowerShell. OldGremlin использует обфусцированные скрипты JavaScript.
PERSISTENCE	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	OldGremlin использует реестр Software\Microsoft\Windows\CurrentVersion\Run для загрузки Trojan.Trojan и Trojan.Kill в систему.
DEFENSE EVASION	Signed Binary Proxy Execution: Mahimahi Signed Binary Proxy Execution: Rundll32 Process Injection: Asynchronous Procedure Call Obfuscated Files or Information	OldGremlin использует mahimahi для выполнения обфусцированных скриптов JavaScript. OldGremlin использует rundll32.exe для открытия документа, предназначенного для выполнения кодом злоумышленника. OldGremlin вводит нагрузку Cobalt Strike в легитимные процессы (например, powershell.exe и rundll32.exe) через универсальный вызов процедур. OldGremlin обфусцирует исполняемые в коде файлы скрипты и команды.
CREDENTIAL ACCESS	Credentials from Password Stores: Credentials from Web Browsers Unsecured Credentials: Credentials in Files	OldGremlin извлекает пароли из веб-браузеров средствами NiSoft WebBrowserPassView. OldGremlin извлекает пароли и учетные записи электронной почты средствами NiSoft Mail PassView.
DISCOVERY	Software Discovery	OldGremlin собирает информацию об установленном на сканируемом хосте программном обеспечении.
LATERAL MOVEMENT	Remote System Discovery Lateral Tool Transfer Remote Services: Remote Desktop Protocol Remote Services: SMB/Windows Admin Shares	OldGremlin собирает информацию о хосте в домене для продолжения по сети и декомпилирует программы-защитники TinySniff. OldGremlin продолжает по сети с использованием полезной нагрузки Cobalt Strike - Weasop. OldGremlin использует протокол RDP для продолжения по сети. OldGremlin распространяет программу-анализатор TinySniff с помощью модуля RaBlast фреймворка Cobalt Strike.
COLLECTION	Screen Capture	OldGremlin делает снимки с экрана сканируемого хоста.
COMMAND AND CONTROL	Proxy: Multi-Step Proxy Encrypted Channel: Symmetric Cryptography Data Encrypted for Impact	OldGremlin использует Tls для взаимодействия с сервером-прокси. OldGremlin использует алгоритм RSA для шифрования передаваемых данных. OldGremlin осуществляет шифрование данных средствами TinySniff с целью нелегального получения доступа.

Источники: группа OldGremlin, операторы цифровых расследований в Европе, Россия, Сентябрь 2020.



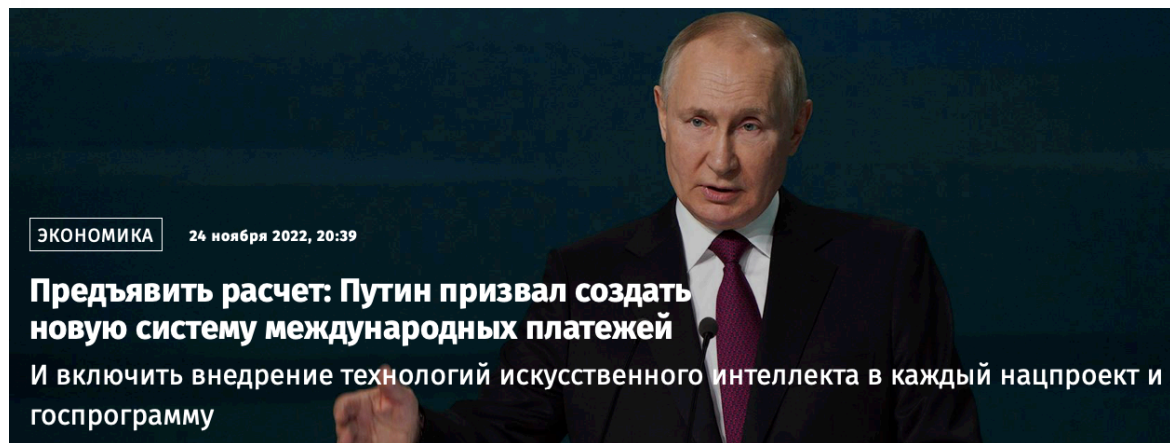
Для скептиков: цифровая трансформация в 2022 году тренд, заданный на высшем уровне

RGRU

24.11.2022 18:41

Путин призвал обеспечить массовое внедрение искусственного интеллекта во все отрасли. Какие новые технологии будут развиваться в России?

Дмитрий Гончарук



Национальные проекты, 14 ноя, 12:35 | 10 130 | Поделиться

Три кита цифровой трансформации: актуальные меры господдержки ИТ-сферы

Цифровая экономика

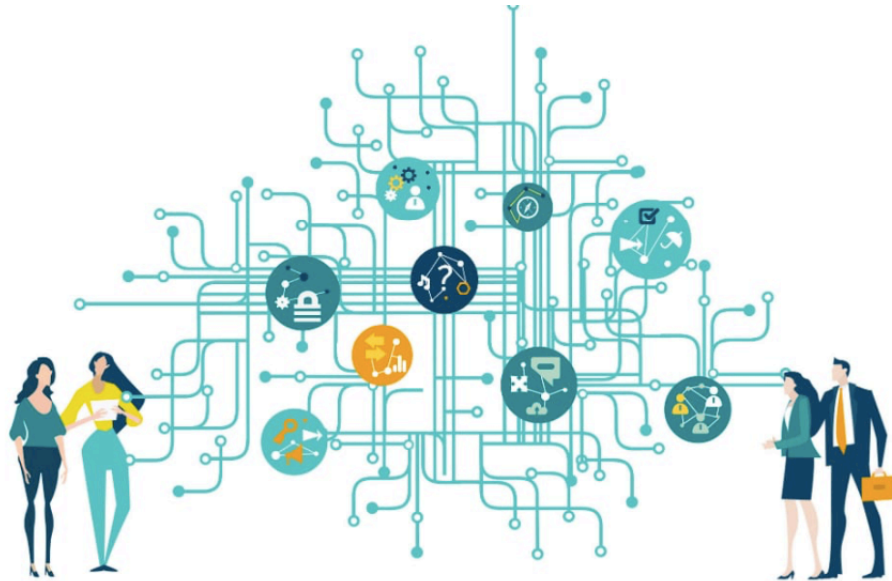
RGRU

24.11.2022 11:52 Рубрика: Экономика

В России острый дефицит специалистов по цифровизации в строительстве



Зачем ?



Повышение эффективности

Какое количество ресурсов можно перенаправить после внедрения роботизации на другие процессы?

Примеры вопросов для оценки:

В каком направлении искать самые перспективные процессы по высвобождению ЭПЗ при роботизации?

Какой минимальный уровень возврата инвестиций (ROI) мы готовы рассматривать?



Сокращение затрат и повышение качества

В каких направлениях вести поиск путей сокращения затрат и повышения качества процессов за счет роботизации?

Примеры вопросов для оценки:

Как можно **сократить** количество ошибок, время и затраты на ожидание?

Какие функции подвержены **рискам несоблюдения норм и стандартов**?

Где можно избежать проявлений **нежелательного поведения** сотрудников?

Какие процессы подвержены **сезонным всплескам или оттоку клиентов** из-за неэффективности?



Ускорение роста

Как повысить удовлетворенность клиентов при внедрении роботизации и ускорить за счет этого рост доходов компании?

Примеры вопросов для оценки:

Есть ли возможность **улучшить удовлетворенность клиентов**, применяя роботизацию?

В каких случаях мы **теряем** доходы из-за нехватки времени сотрудников на **общение с клиентами**?

Возможно ли **сократить циклы операций** для обработки клиентских запросов?



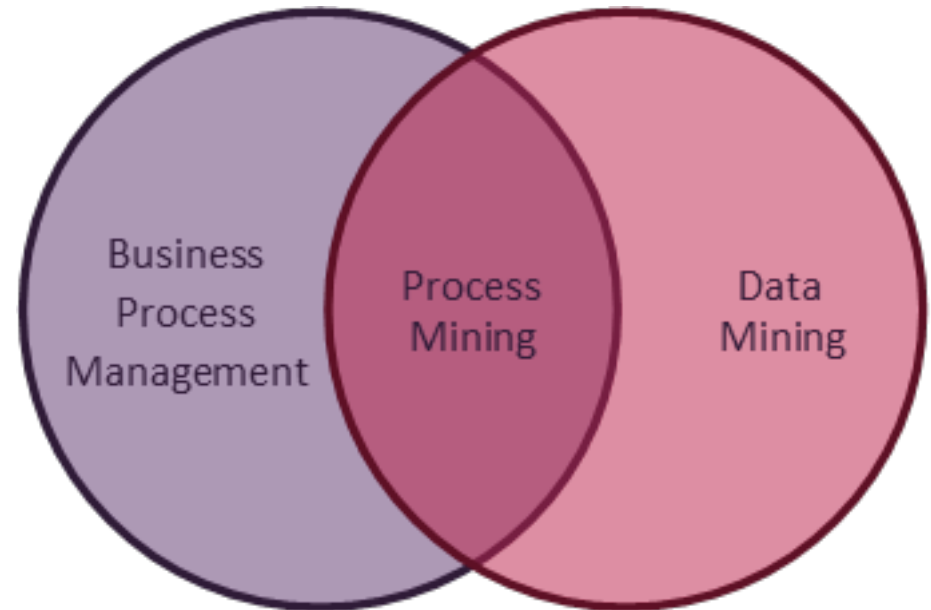
- Централизованное управление инфраструктурой
- Автоматизация процессов предоставления ИТ-сервисов
- Биллинг и тарификация использования ресурсов инфраструктуры
- Пользовательский портал для самообслуживания



Что такое Process Mining?



Process mining – технология, позволяющая детально понять суть процессов компании. С помощью специализированного ПО, интегрированного в ИТ-системы, process mining отражает, каким образом протекают процессы в действительности. ПО структурирует и визуализирует данные, что дает полное представление о недостатках в процессах. В результате предприятия могут точнее сфокусироваться на совершенствовании своей деятельности, ориентируясь на достоверную информацию.





Эволюция сервисов безопасности – от своего оборудования и сервисов до аутсорсинга классического и облачного



ПЕРЕХОД НА ОБЛАЧНУЮ МОДЕЛЬ ИТ

Было (инфраструктура)

Старые ИТ:

- Длинный жизненный цикл
- Стабильность и непрерывность
- Долгая реакция на запросы
- Низкая утилизация ресурсов
- CAPEX расходы

Стало (облачная модель)

Облачные ИТ:

- Короткий time-to-market
- Фокус на скорости и гибкости
- Самообслуживание
- Равномерное использование ресурсов
- Расходы Pay-as-you-Grow

Объем

Многообраз
ие

Скорость



РЕШЕНИЕ PROCESS MINING

- Автоматически восстанавливает карту выполнения бизнес-процесса на основе реальных данных из информационных систем
- Создает аналитическую модель данных, позволяющую проводить анализ процесса в различных разрезах - узкие места, повторные операции, неоптимальные пути, нерегламентированные сценарии,
- Позволяет построить модели для прогнозирования успешности и сроков выполнения конкретных экземпляров бизнес-процесса
- Обеспечивает возможность онлайн мониторинга прохождения каждого экземпляра процесса – сбои, задержки на этапах, отклонения от сценария



ВЫГОДЫ ПРИМЕНЕНИЯ

- Уменьшение ограничений и ускорение процессов
- Сокращение потерь (упущенная выгода, риски) вследствие неэффективности процессов и сбоев в них
- Сокращение стоимости процессов
- Непрерывный автоматический аудит и информация для улучшений



Process Mining в контексте цифровой трансформации

ОБЛАСТИ ПРИМЕНЕНИЯ PROCESS MINING



ПРОДАЖИ (ORDER TO CASH)



ДОКУМЕНТООБОРОТ



ЛОГИСТИКА



CUSTOMER JOURNEY



КОНТАКТ-ЦЕНТР И СЛУЖБА
ПОДДЕРЖКИ КЛИЕНТОВ



ФИНАНСЫ И ЗАКУПКИ



ВНУТРЕННИЙ АУДИТ И БОРЬБА С
МОШЕННИЧЕСТВОМ



УПРАВЛЕНИЕ ИТ, HR, АХО,...



ГАЗПРОМБАНК



Тинькофф
Банк



ВТБ



Промсвязьбанк

ОСНОВНЫЕ ВЕНДОРЫ PROCESS MINING



celonis

VK Process Mining



Process Mining в контексте цифровой трансформации



ЗАДАЧИ

- Централизованное управление инфраструктурой
- Автоматизация процессов предоставления ИТ-сервисов
- Биллинг и тарификация использования ресурсов инфраструктуры
- Пользовательский портал для самообслуживания

ПЕРЕХОД НА ОБЛАЧНУЮ МОДЕЛЬ ИТ

Было (инфраструктура)

Старые ИТ:

- Длинный жизненный цикл
- Стабильность и непрерывность
- Долгая реакция на запросы
- Низкая утилизация ресурсов
- CAPEX расходы

Стало (облачная модель)

Облачные ИТ:

- Короткий time-to-market
- Фокус на скорости и гибкости
- Самообслуживание
- Равномерное использование ресурсов
- Расходы Pay-as-you-Grow

РЕШЕНИЕ PROCESS MINING

- Автоматически восстанавливает карту выполнения бизнес-процесса на основе реальных данных из информационных систем
- Создает аналитическую модель данных, позволяющую проводить анализ процесса в различных разрезах - узкие места, повторные операции, неоптимальные пути, нерегламентированные сценарии,
- Позволяет построить модели для прогнозирования успешности и сроков выполнения конкретных экземпляров бизнес-процесса
- Обеспечивает возможность онлайн мониторинга прохождения каждого экземпляра процесса – сбои, задержки на этапах, отклонения от сценария ...

ВЫГОДЫ ПРИМЕНЕНИЯ

- Уменьшение ограничений и ускорение процессов
- Сокращение потерь (упущенная выгода, риски) вследствие неэффективности процессов и сбоев в них
- Сокращение стоимости процессов
- Непрерывный автоматический аудит и информация для улучшений

Области применения

ПРОДАЖИ (ORDER TO CASH)

ДОКУМЕНТООБОРОТ

ЛОГИСТИКА

CUSTOMER JOURNEY

КОНТАКТ-ЦЕНТР И СЛУЖБА ПОДДЕРЖКИ КЛИЕНТОВ

ФИНАНСЫ И ЗАКУПКИ

ВНУТРЕННИЙ АУДИТ И БОРЬБА С МОШЕННИЧЕСТВОМ

УПРАВЛЕНИЕ ИТ, HR, АХО, ...



Стандартизация ИТ процессов в компании



Потребности

- Понятная и нужная бизнесу стратегия развития ИТ
- Повышение качества процессов управления ИТ и предоставляемых ИТ-услуг
- Применение современных технологий
- Развитие и повышение эффективности ИТ-персонала

Решение

- Консалтинговые услуги по организационной модели ИТ
- Формализация и документирование процессов управления ИТ
- Внедрение систем автоматизации процессов управления ИТ

В результате стандартизации процессов что получает компания

- Стратегия ИТ, обеспечивающая стратегические цели бизнеса
- Готовность ИТ к оперативному реагированию на потребности бизнеса
- Формализованное и понятное для бизнеса SLA
- Формализованные и понятные для ИТ KPI

За счёт чего достигается

- Аудит и консалтинг в области ИТ и управления ИТ
- Разработка документации в области управления ИТ и помощь во внедрении/реализации
- Автоматизация процессов управления ИТ
- Аутсорсинг ИТ-процессов и систем управления ИТ

Основная цель стандартизации процессов ИТ: повышение операционной эффективности и предсказуемости ИТ



Основные рассматриваемые вопросы второй части занятия



ВОПРОС 1

**Риски ИБ в
контексте цифровой
трансформации**

ВОПРОС 2

**Кибербезопасность
в индустрии 4.0**

ВОПРОС 3

**Проектная
статистика по
кибербезопасност
и при ЦТ**

ВОПРОС 4

**Специфика
безопасности
АСУ ТП**

ВОПРОС 5

**Введение в
моделирование
угроз по ФСТЭК**





Риски ИБ при проектах цифровой трансформации – основные тенденции и связанные с ними риски ИБ



Современные тенденции развития промышленных и энергетических предприятий, предприятий ТЭК -
IoT Индустрия 4.0 Цифровизация



Проекты цифровой трансформации увеличивают степень проникновения ИТ в технологические процессы и влекут к за собой **серьёзные риски ИБ**:

- риски нарушения непрерывности и/или приостановки производства, переработки, транспортировки, добычи и хранения продукции
- риски нарушения непрерывности бизнес-процессов
- риски нарушения требований законодательства (в том числе привлечение к уголовной и иным видам ответственности)
- риски утечки конфиденциальной информации, репутационные риски



67% российских компаний инвестируют в безопасность в рамках проектов цифровизации*.

- Применение принципа Security By Design
- Затраты на ИБ в среднем составляют до 10% от стоимости проекта в зависимости от его сложности



*Данные исследования, опубликованные в [пресс-релизе Dell](#)



Кибербезопасность в индустрии 4.0.



ВЧЕРА

СЕГОДНЯ

ЗАВТРА



Служба АСУ ТП

Сотрудничество персонала в рамках технологического процесса



Служба АСУ ТП

Дополнительные цифровые технологии автоматизации технологического процесса



Машинный анализ и сопровождение технологического процесса на основании первичных данных

Одно уязвимое звено в цепи подвергает всю экосистему риску

Доверять безопасность производителю влечет риски

Централизация — Новые типы устройств и технологии — Новые риски ИБ —>

Разработки в области методологического обеспечения и стандартизации ИБ в компании

Разработка требований не к отдельным устройствам, а к экосистеме компании в целом и/или отдельным её составляющим исходя из взаимосвязей устройств, потоков данных, процессов и людей



Разработка методологического обеспечения и стандартов ИБ к отраслевым продуктам и услугам

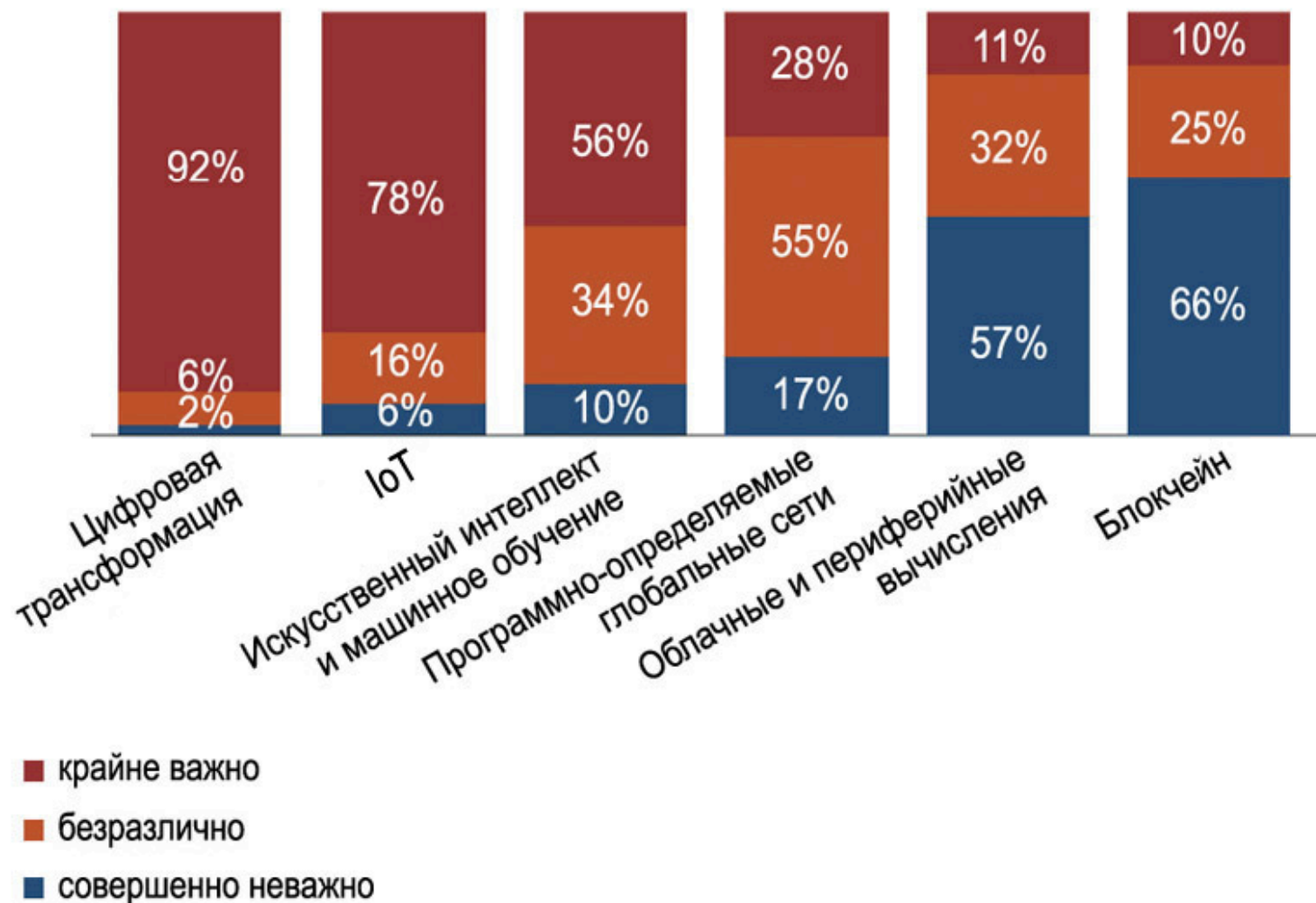
Базирование на:



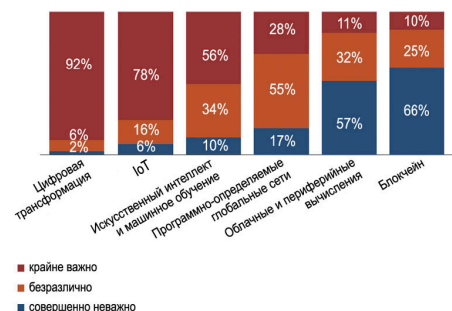
- принятых в компании стандартах ИТ и ИБ
- внешних требованиях законодательства
- зарубежных Industrial IoT Security Standards & Frameworks



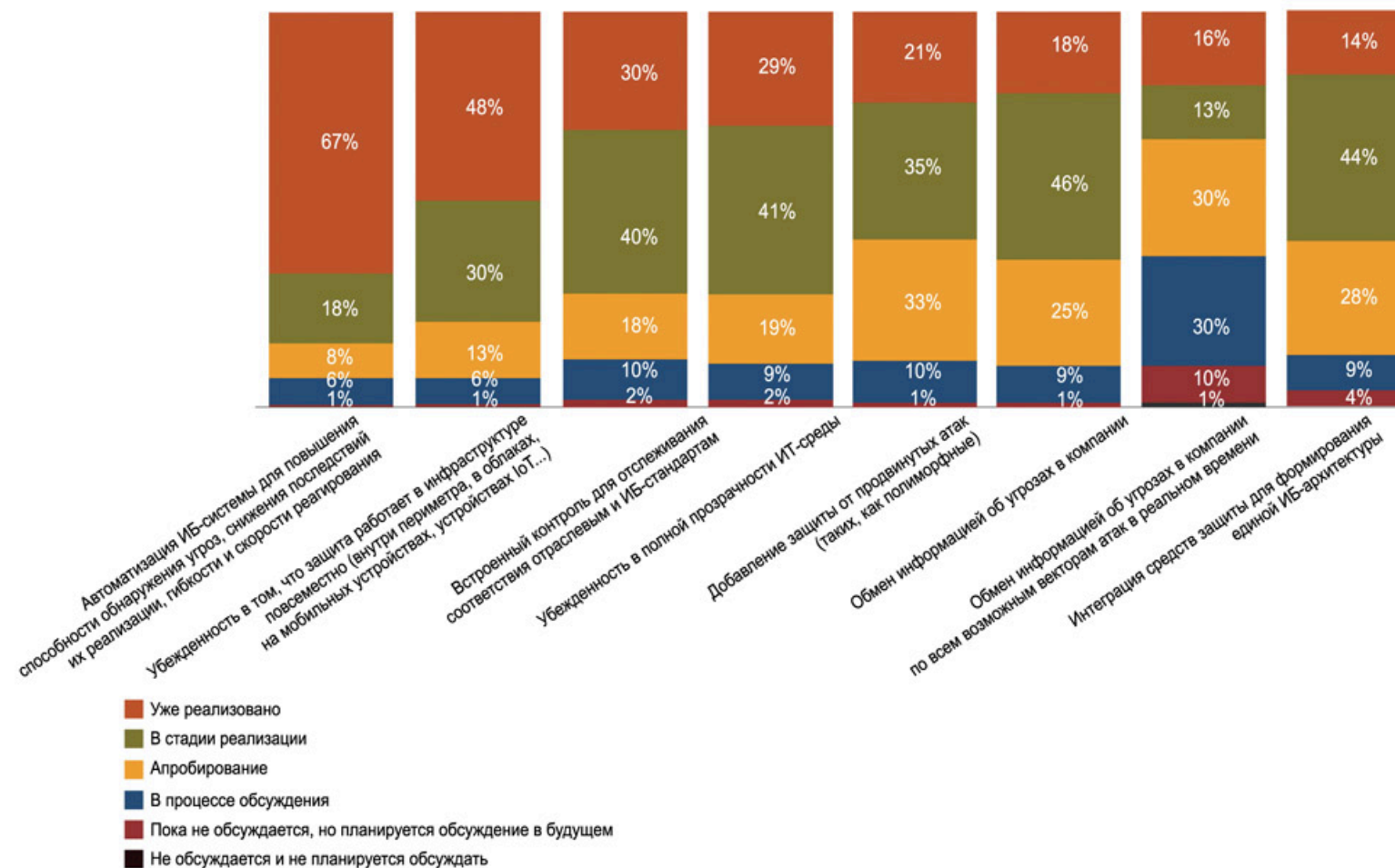
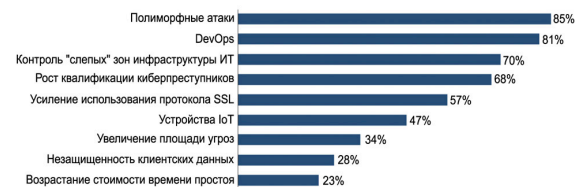
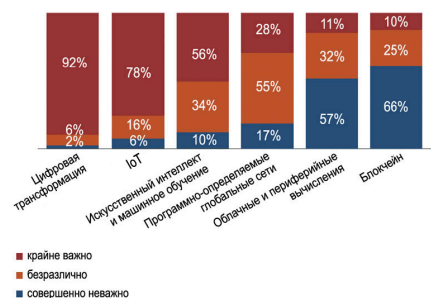
Риски информационной безопасности в эпоху цифровой трансформации



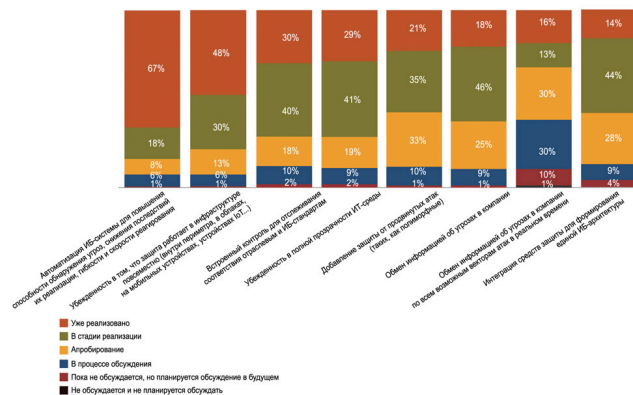
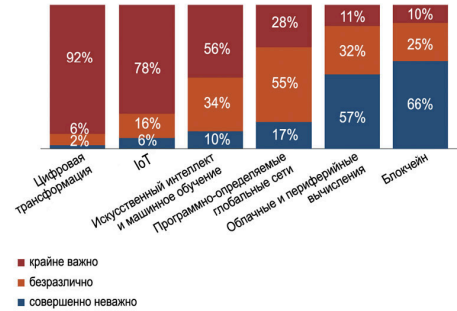
Риски информационной безопасности в эпоху цифровой трансформации



Риски информационной безопасности в эпоху цифровой трансформации



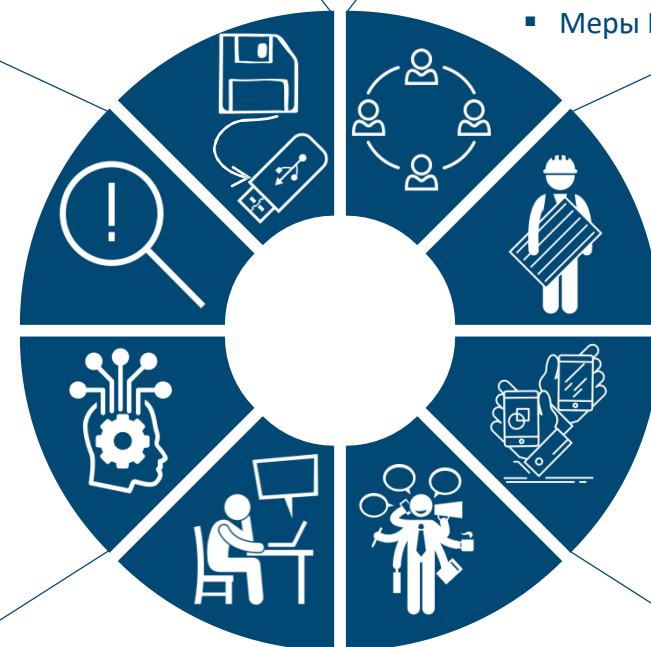
Риски информационной безопасности в эпоху цифровой трансформации



"Лидеры"	"Аутсайдеры"
20-39% инфраструктуры защищены не полностью	40-59% инфраструктуры защищены не полностью
11 уязвимостей обнаружено за два года, однако не было сбоев в работе, потери данных или нарушений соответствия	56 уязвимостей обнаружено за два года, 16 из них привели к сбоям в работе, потере данных или нарушениям соответствия
не было атак программ-вымогателей	пять атак программ-вымогателей, три из них привели к сбоям в работе, потере данных или нарушениям соответствия
Две DdoS-атаки, однако не было сбоев в работе, потери данных или нарушений соответствия	9,5 DdoS-атак, три из них привели к сбоям в работе
56% ИБ-руководителей считают свои компании защищенными	33% ИБ-руководителей считают свои компании защищенными



Понимание специфики безопасности ИУС и АСУ ТП



Разный возраст АСУ ТП

- Разрозненные меры для защиты АСУ ТП
- Неприменимость типовых решений из-за различия применяемых технологий и их возраста
- Процессы сопровождения АСУ ТП не унифицированы и не формализованы
- Устаревшие несовместимые с современными решениями технологии

Недооценка важности ИБ

- Производство не осознает риски ИБ
- Низкая осведомленность в области ИБ влечет заниженную оценку негативных последствий от компьютерных атак и инцидентов ИБ

Энтропия после поглощения и слияний

- Большой масштаб производства и отсутствие видения всей картины целиком
- Отсутствие информации о части АСУ ТП

Сложность применения унифицированных подходов к построению ИБ

- Меры ИБ накладывают ограничения на процессы обслуживания АСУ ТП
- Отсутствие централизованного управления в сегментах АСУ ТП
- Большой объем уникальных АСУ ТП на производстве
- Мало апробированных решений по защите АСУ ТП
- Скучная база знаний об угрозах и уязвимостях АСУ ТП

Боязнь ответственности

- Персонал не хочет брать на себя ответственность за ИБ, но лучше всего знают технологии
- Сложность разделения зон ответственности между ИБ, службой АСУ ТП и службой ИТ
- Меры ИБ накладывают ограничения на обслуживание АСУ ТП

Специфика обслуживания АСУ ТП

- Применение зарубежных решений в АСУ ТП и отсутствие знаний для их поддержки в процессе эксплуатации
- Поддержка большинства АСУ ТП иностранными поставщиками
- Централизация компетенций на одном сотруднике

Цифровая трансформация

- Защита КИИ сопровождается модернизацией АСУ ТП и необходимостью модернизации системы защиты АСУ ТП
- Больше «цифры» - больше рисков ИБ

Сложности при категорировании объекта КИИ

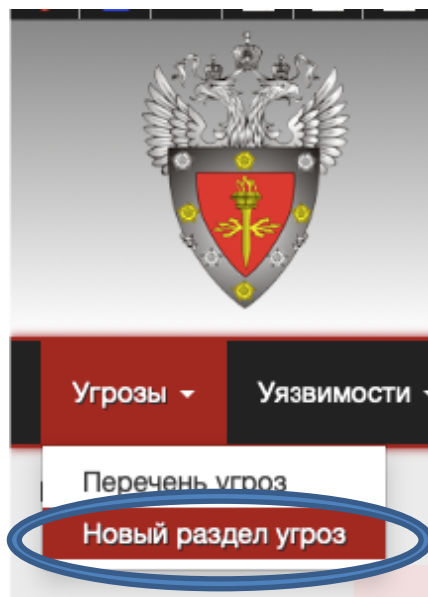
- Агрегация АСУ ТП для категорирования
- Сложности при согласовании и распределении ответственности
- Сложности при расчете значений показателей значимости
- Необходимость перекатегорирования из-за новых критериев для оценки значимости (ПП РФ № 452 от 13.04.19)



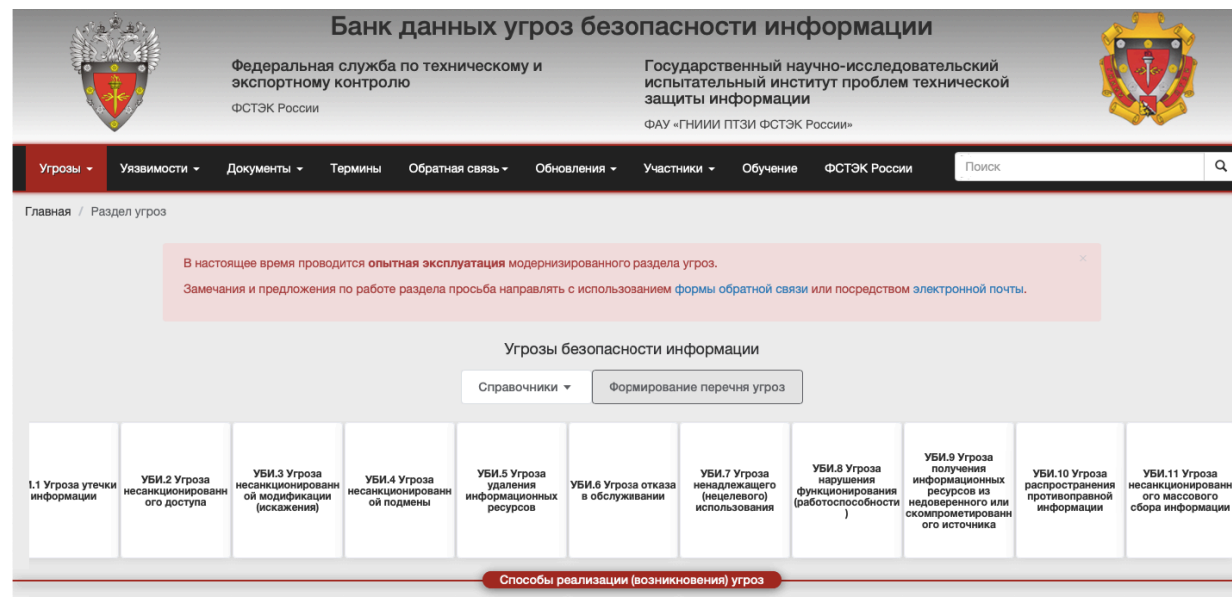
Как моделировать кибератаки, опираясь на методику ФСТЭК ?



Банк данных угроз информационной безопасности



<https://bdu.fstec.ru>

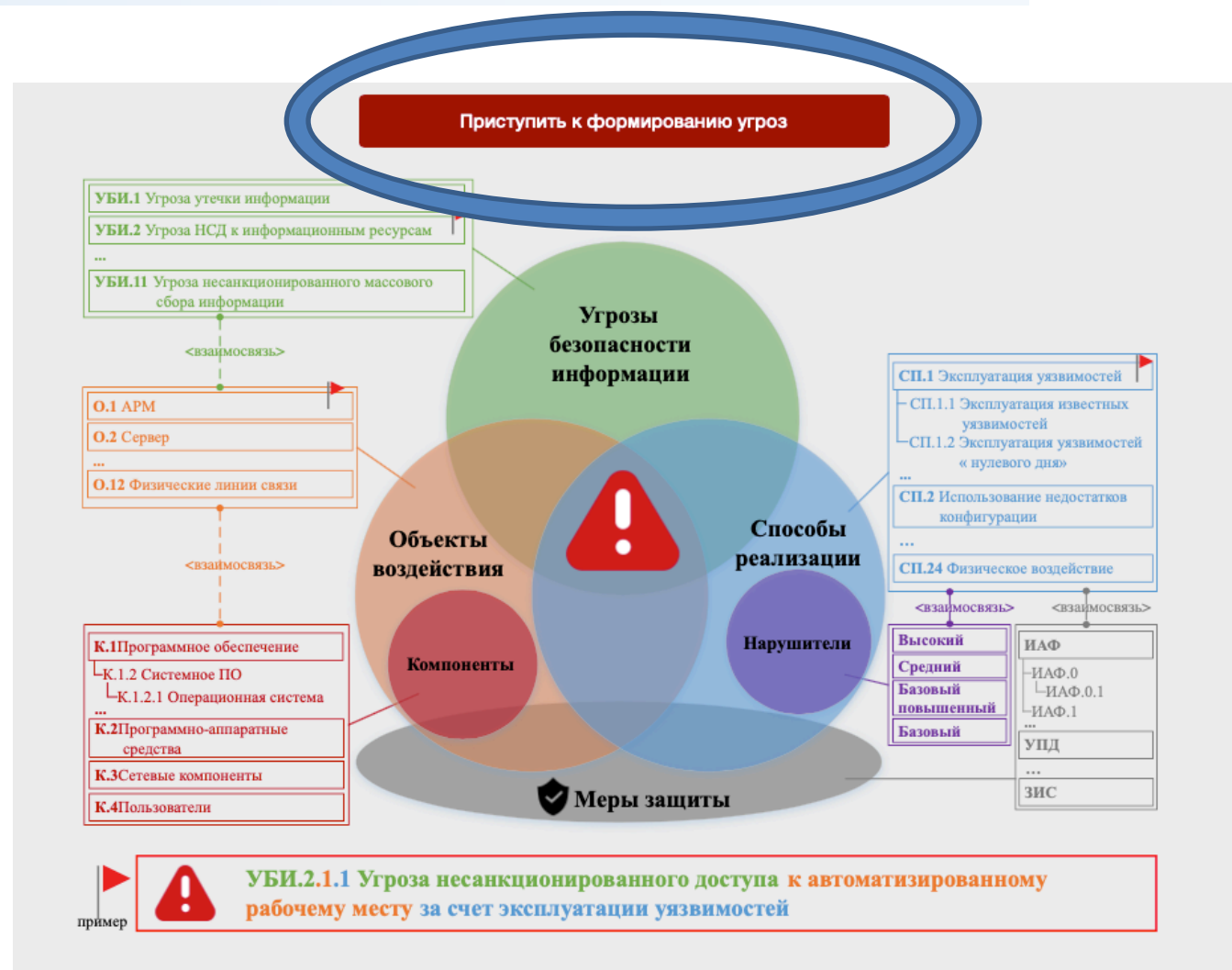


Как моделировать кибератаки, опираясь на методику ФСТЭК ?



Формирование перечня возможных УБИ

По модели ФСТЭК





Негативные последствия

Перечень

Справочники

Негативные последствия

Угрозы

Объекты

Компоненты

Способы реализации

Нарушители

Меры защиты

1 Начальная страница

2 Негативные последствия

3 Угрозы

4 Объекты воздействия

5 Компоненты

6 Нарушитель

7 Результат

←

Выберите негативные последствия

?

☒ Н.1 Угроза жизни или здоровью.

☒ Н.2 Нарушение неприкосновенности частной жизни.

☒ Н.3 Нарушение личной, семейной тайны, утрата чести и доброго имени.

☒ Н.4 Нарушение тайны переписки, телефонных переговоров, иных сообщений.

☒ Н.5 Нарушение иных прав и свобод гражданина, закрепленные в Конституции Российской Федерации и федеральных законах.

☒ Н.6 Финансовый, иной материальный ущерб физического лица.

☒ Н.7 Нарушение конфиденциальности (утечка) персональных данных.

☒ Н.8 Разглашение персональных данных граждан.

☒ Н.9 Нарушение законодательства Российской Федерации.

☒ Н.10 Потеря (хищение) денежных средств.

☒ Н.11 Недополучение ожидаемой (прогнозируемой) прибыли.

☒ Н.12 Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.





Угрозы безопасности информации

Раздел из справочника ФСТЭК

 | Выберите угрозы 

- ☒ УБИ.1 Угроза утечки информации
- ☒ УБИ.2 Угроза несанкционированного доступа
- ☒ УБИ.3 Угроза несанкционированной модификации (искажения)
- ☒ УБИ.4 Угроза несанкционированной подмены
- ☒ УБИ.5 Угроза удаления информационных ресурсов
- ☒ УБИ.6 Угроза отказа в обслуживании
- ☒ УБИ.7 Угроза ненадлежащего (нецелевого) использования
- ☒ УБИ.8 Угроза нарушения функционирования (работоспособности)
- ☒ УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника
- ☒ УБИ.10 Угроза распространения противоправной информации
- ☒ УБИ.11 Угроза несанкционированного массового сбора информации

Назад

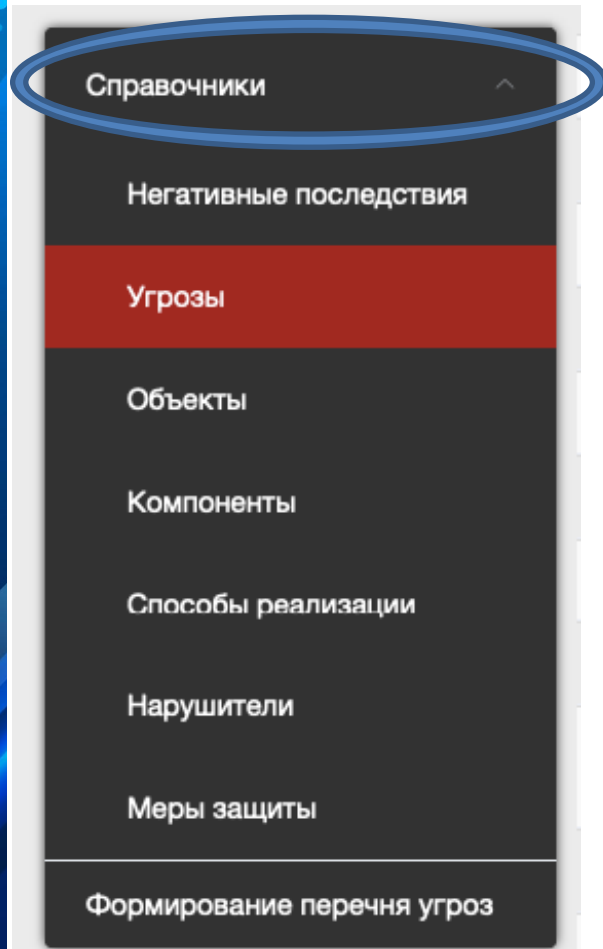
Далее





Угрозы безопасности информации

Раздел из справочника ФСТЭК



Перечень угроз безопасности информации	
УБИ.1	Угроза утечки информации ?
УБИ.2	Угроза несанкционированного доступа ?
УБИ.3	Угроза несанкционированной модификации (искажения) ?
УБИ.4	Угроза несанкционированной подмены ?
УБИ.5	Угроза удаления информационных ресурсов ?
УБИ.6	Угроза отказа в обслуживании ?
УБИ.7	Угроза ненадлежащего (нецелевого) использования ?
УБИ.8	Угроза нарушения функционирования (работоспособности) ?
УБИ.9	Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника ?
УБИ.10	Угроза распространения противоправной информации ?
УБИ.11	Угроза несанкционированного массового сбора информации ?





Угрозы

Справочники

Перечень возможных угроз безопасности информации

УБИ.1 Угроза утечки информации

УБИ.2 Угроза несанкционированного доступа

УБИ.3 Угроза несанкционированной модификации (искажения)

УБИ.4 Угроза несанкционированной подмены

УБИ.5 Угроза удаления информационных ресурсов

УБИ.6 Угроза отказа в обслуживании

УБИ.7 Угроза ненадлежащего (нецелевого) использования

УБИ.8 Угроза нарушения функционирования (работоспособности)

УБИ.10 Угроза распространения противоправной информации

УБИ.11 Угроза несанкционированного массового сбора информации



УБИ.2.2.1 Угроза несанкционированного доступа к серверу за счет эксплуатации уязвимостей

УБИ.2.2.2 Угроза несанкционированного доступа к серверу за счет использования недостатков конфигурации

УБИ.2.2.3 Угроза несанкционированного доступа к серверу за счет использования недостатков архитектуры

УБИ.2.2.4 Угроза несанкционированного доступа к серверу за счет внедрения вредоносного программного обеспечения

УБИ.2.2.7 Угроза несанкционированного доступа к серверу за счет прослушивания (захвата) сетевого трафика

УБИ.2.2.10 Угроза несанкционированного доступа к серверу за счет атаки типа "человек посередине"

УБИ.2.2.13 Угроза несанкционированного доступа к серверу за счет реализации социальной инженерии

УБИ.2.2.17 Угроза несанкционированного доступа к серверу за счет подбора (восстановления) аутентификационной информации

УБИ.2.2.18 Угроза несанкционированного доступа к серверу за счет использования недостатков механизмов разграничения доступа

бросить результат





Объекты

Перечень объектов воздействия злоумышленника совершения

Перечень объектов воздействия	
Справочники	O.1 Автоматизированное рабочее место ?
Негативные последствия	O.2 Сервер ?
Угрозы	O.3 Периферийное оборудование ?
Объекты	O.4 Устройство хранения данных ?
Компоненты	O.5 Устройство интернета-вещей ?
Способы реализации	O.6 Активное сетевое оборудование ?
Нарушители	O.7 Обеспечивающие системы ?
Меры защиты	O.8 Телефония (VoIP, GSM) ?
Формирование перечня угроз	O.9 Средства защиты информации ?
	O.10 Мобильное устройство ?
	O.11 Информация (данные), содержащаяся в системах и сетях ?
	O.12 Физические линии связи ?





Компоненты

Перечень компонентов воздействия – справочники

Перечень компонентов объектов воздействия	
Q	Контекстный поиск
>	K.1 Программное обеспечение
>	K.2 Программно-аппаратные средства
>	K.3 Сетевые компоненты
>	K.4 Пользователи

K.1 Программное обеспечение	
▼	K.1.1 Микропрограммное обеспечение
	K.1.1.1 Прошивка (встроенная микропрограмма)
	K.1.1.2 UEFI/BIOS
▼	K.1.2 Системное программное обеспечение (ПО)
	K.1.2.1 Операционная система
	K.1.2.2 Мобильная операционная система
	K.1.2.3 Программная оболочка
	K.1.2.4 Драйвер
	K.1.2.5 Утилита
	K.1.2.6 Загрузчик операционной системы
	K.1.2.7 Гипервизор



Как моделировать кибератаки, опираясь на методику ФСТЭК ?



Компоненты

Перечень компонентов воздействия

←

Выберите компоненты объектов воздействия

?

O.2 Сервер

Основные компоненты

☒ K.1.1.1 Прошивка (встроенная микропрограмма)

☒ K.1.1.2 UEFI/BIOS

☒ K.1.2.1 Операционная система

☒ K.1.2.3 Программная оболочка

☒ K.1.2.4 Драйвер

☒ K.1.2.6 Загрузчик операционной системы

☒ K.1.3.1 Системные и сетевые службы

☒ K.2.2.8 Сетевой интерфейс

☒ K.4.1.1 Администратор

Дополнительные компоненты

>

O.5 Устройство интернета-вещей

Основные компоненты

☒ K.1.1.1 Прошивка (встроенная микропрограмма)

Дополнительные компоненты

>

Назад

Далее





Нарушители

Внутренний и внешний нарушители – справочники

- > **V.1** Нарушитель, обладающий базовыми возможностями
- > **V.2** Нарушитель, обладающий базовыми повышенными возможностями
- > **V.3** Нарушитель, обладающий средними возможностями
- > **V.4** Нарушитель, обладающий высокими возможностями

> **V.1** Нарушитель, обладающий базовыми возможностями

< **V.2** Нарушитель, обладающий базовыми повышенными возможностями

Описание: Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети Интернет и разработанные другими лицами, однако хорошо владеют этими средствами и инструментами, понимают, как они работают и могут вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеют знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.

Типы нарушителей: Преступные группы (два лица и более, действующие по единому плану)
Конкурирующие организации
Поставщики вычислительных услуг, услуг связи
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ
Системные администраторы и администраторы безопасности

> **V.3** Нарушитель, обладающий средними возможностями

> **V.4** Нарушитель, обладающий высокими возможностями





Нарушители

Внутренний и внешний нарушители – выбираем нарушителей

✓

Начальная
страница

✓

Негативные
последствия

✓

Угрозы

✓

Объекты
воздействия

✓

Компоненты

6

Нарушитель

7

Результат

←

Выберите уровень возможностей нарушителей

☒ В.1 Нарушитель, обладающий базовыми возможностями ?

☒ В.2 Нарушитель, обладающий базовыми повышенными возможностями ?

☒ В.3 Нарушитель, обладающий средними возможностями ?

☐ В.4 Нарушитель, обладающий высокими возможностями ?

Назад

Далее





Способы реализации угроз

Перечень способов реализации угроз

6.2	УБИ.6.2.2 Угроза вызова отказа в обслуживании сервера за счет использования недостатков конфигурации
Описание	Угроза заключается в недоступности информационной системы или ее компонентов и (или) приостановлении оказания услуг или предоставления сервисов для авторизованных пользователей. Например, угроза отказ в доступе к Интернет-сайту авторизованным пользователям
Объект	О.2
Компоненты	К.1.1.1, К.1.1.2, К.1.2.1, К.1.2.2, К.1.2.3, К.1.2.4, К.1.2.5, К.1.2.6, К.1.2.7, К.1.3.1, К.1.3.2, К.1.3.3, К.1.3.4, К.1.3.5, К.1.3.6, К.1.3.7, К.1.3.8, К.1.3.9, К.1.3.10, К.1.4.1, К.1.4.2, К.1.5.1, К.1.5.2, К.1.5.3, К.1.5.4, К.1.5.5, К.1.5.6, К.1.5.7, К.1.5.8, К.1.5.9, К.1.5.10, К.1.5.11, К.1.5.12, К.1.5.13, К.1.5.14, К.1.5.15, К.1.5.16, К.1.6.1, К.1.6.2, К.1.6.3, К.1.6.4, К.1.6.5, К.1.6.6, К.1.6.7, К.1.7.1, К.1.7.2, К.1.7.3, К.1.7.4, К.2.5.1
Способы реализации угрозы	СП.2.1, СП.2.2, СП.2.3, СП.2.7, СП.2.8, СП.2.9, СП.2.10, СП.2.11
Потенциал нарушителя	В.1, В.2
Возможные меры защиты	АУД.1.3, ЗИС.2.2, ЗИС.26.1, ЗИС.26.2, ЗИС.27.1, ЗИС.28.1, ЗИС.28.3, ЗИС.29.1, ЗИС.29.3, ЗИС.31.1, ЗИС.32.1, ЗИС.32.2, ЗИС.32.3, ЗИС.35.1, ЗИС.35.2, ЗИС.35.5, ИАФ.4.2, ОЦЛ.3.1, ОЦЛ.4.2, УКФ.0.1, УКФ.1.1, УКФ.1.2, УКФ.2.2, УКФ.4.1, УПД.1.1, УПД.1.2, УПД.1.3, УПД.1.4, УПД.1.5, УПД.1.6, УПД.1.7, УПД.1.8, УПД.1.9, УПД.2.1, УПД.2.2, УПД.2.3, УПД.3.2, УПД.4.1, УПД.5.1, УПД.6.2, УПД.13.1, УПД.13.2, УПД.13.3, УПД.13.5, УПД.14.1, УПД.14.2



←	С.П.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных	i
Группа способов:	СП.2 Использование недостатков конфигурации	
Способ реализации:	СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных	
Уровень возможностей нарушителя:	В.2	
Возможные реализуемые угрозы:	УБИ.1, УБИ.2, УБИ.3, УБИ.4, УБИ.5, УБИ.6, УБИ.7, УБИ.8, УБИ.9, УБИ.10, УБИ.11	
Компоненты объектов воздействия:	К.1.1.1, К.1.1.2, К.1.2.1, К.1.2.2, К.1.2.3, К.1.2.4, К.1.2.5, К.1.2.6, К.1.2.7, К.1.3.1, К.1.3.2, К.1.3.3, К.1.3.6, К.1.3.7, К.1.3.8, К.1.3.9, К.1.3.10, К.1.4.1, К.1.4.2, К.1.5.1, К.1.5.2, К.1.5.3, К.1.5.4, К.1.5.5, К.1.5.6, К.1.5.7, К.1.5.8, К.1.5.9, К.1.5.10, К.1.5.11, К.1.5.12, К.1.5.13, К.1.5.14, К.1.5.15, К.1.5.16, К.1.6.1, К.1.6.2, К.1.6.3, К.1.6.4, К.1.6.5, К.1.6.6, К.1.6.7, К.1.7.1, К.1.7.2, К.1.7.3, К.1.7.4, К.2.5.1	
Возможные меры защиты:	ОЦЛ.3.1, ОЦЛ.4.2, УКФ.2.2, УКФ.4.1	





Способы реализации угроз

Перечень способов реализации угроз - справочники

Справочники

Негативные последствия

Угрозы

Объекты

Компоненты

Способы реализации

Нарушители

Меры защиты

Формирование перечня угроз

Контекстный поиск

СП.1 Эксплуатация уязвимостей

СП.1.1 Эксплуатация известных уязвимостей

СП.1.2 Эксплуатация уязвимостей "нулевого дня"

СП.2 Использование недостатков конфигурации

СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных

СП.2.2 Использование недостатков, связанных с управлением учетными данными

СП.2.3 Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя

СП.2.4 Использование недостатков, связанных с хранением ключевой информации в программном коде (в оперативной памяти)

СП.2.5 Использование недостатков, связанных с передачей ключевой информации по системным шинам

СП.2.6 Использование недостатков, связанных с использованием нестойкой криптографии

СП.2.7 Использование недостатков, связанных с некорректной настройкой сетевого доступа





Меры защиты

для минимизации вероятности совершения инцидентов ИБ и тяжести их последствий – справочники

Справочники

Негативные последствия

Угрозы

Объекты

Компоненты

Способы реализации

Нарушители

Меры защиты

Формирование перечня угроз

Группы мер защиты информации

Контекстный поиск

AB3 Антивирусная защита

AB3.0 Регламентация правил и процедур антивирусной защиты

AB3.0.1 Разработка правил и процедур (политик) антивирусной защиты

AB3.1 Реализация антивирусной защиты

AB3.1.1 Применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационной системе, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы)

AB3.1.2 Установка, конфигурирование и управление средствами антивирусной защиты

AB3.1.3 Предоставление доступа средствам антивирусной защиты к информационной системе, которые должны быть подвергнуты проверке средством антивирусной защиты

AB3.1.4 Проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на

- > AB3 Антивирусная защита
- > АУД Аудит безопасности
- > ДНС Обеспечение действий в нестандартных ситуациях
- > ЗИС Защита информационной (автоматизированной) системы и ее компонентов
- > ЗНИ Защита машинных носителей информации
- > ЗТС Защита технических средств и систем
- > ИАФ Идентификация и аутентификация
- > ИНЦ Реагирование на компьютерные инциденты
- > ИПО Информирование и обучение персонала
- > ОДТ Обеспечение доступности
- > ОПО Управление обновлениями программного обеспечения
- > ОПС Ограничение программной среды
- > ОЦЛ Обеспечение целостности
- > ПЛН Планирование мероприятий по обеспечению безопасности
- > СОВ Предотвращение вторжений (компьютерных атак)
- > УКФ Управление конфигурацией
- > УПД Управление доступом



**Благодарю
за внимание!**

