Приложение 7. Опросный лист для оценки угроз по методу CRAMM

написано Александр Астахов | 11 июня, 2023

Угроза: **Использование чужого идентификатора сотрудниками организации («маскарад»)**

- Сколько раз за последние 3 года сотрудники организации пытались с использованием прав других пользователей получить несанкционированный доступ к хранящейся в системе (сети) информации?
- Какова тенденция в статистике такого рода попыток несанкционированного проникновения в систему (сеть)?
- Хранится ли в системе (сети) информация (например, личные дела), которая может представлять интерес для сотрудников организации и побуждать их к попыткам несанкционированного доступа к ней?
- Известны ли случаи нападения, угроз, шантажа, давления на сотрудников со стороны посторонних лиц?
- Существуют ли среди персонала группы лиц или отдельные личности с недостаточно высокими моральными качествами?
- Хранится ли в системе (сети) информация, несанкционированное изменение которой может принести прямую выгоду сотрудникам?
- Предусмотрена ли в системе (сети) поддержка пользователей, обладающих техническими возможностями совершить подобную «агрессию»?
- Существуют ли другие способы просмотра информации, позволяющие злоумышленнику добраться до нее более простыми методами, чем с использованием «маскарада»?
- Существуют ли другие способы несанкционированного изменения информации, позволяющие злоумышленнику достичь желаемого результата более простыми методами, чем с

использованием «маскарада»?
- Сколько раз за последние 3 года сотрудники пытались получить несанкционированный доступ к информации, хранящейся в других подобных системах в вашей организации?

Угроза: **Использование чужого идентификатора поставщиками услуг («маскарад»)**

- Сколько раз за последние 3 года поставщики услуг пытались с использованием прав других пользователей получить несанкционированный доступ к хранящейся в системе (сети) информации?
- Хранится ли в системе (сети) информация, которая может представлять интерес для сотрудников фирм-поставщиков услуг, например сведения о заключенных контрактах?
- Используется ли система (сеть) для работы с финансовыми прикладными программами?
- Известны ли случаи нападения, угроз, шантажа, давления на персонал фирмы-поставщика услуг со стороны посторонних лиц?
- Каков общий уровень моральных качеств персонала фирмы-поставщика услуг?
- Какова тенденция в статистике попыток несанкционированного проникновения в систему (сеть) со стороны фирмы-поставщика услуг?

Угроза: **Использование чужого идентификатора посторонними («маскарад»)**

- Какая из нижеперечисленных групп может проявлять повышенный интерес к хранящейся в системе (сети) информации?
- Сколько раз за последние 3 года посторонние лица пытались с использованием прав пользователей получить несанкционированный доступ к хранящейся в системе (сети)

информации?

- Какова общая тенденция в статистике подобных попыток?
- Может ли раскрытие хранящейся в системе (сети) информации принести прямую финансовую выгоду посторонним лицам?
- Может ли искажение хранящейся в системе (сети) информации принести прямую финансовую выгоду посторонним лицам?
- Может ли сокрытие хранящейся в системе (сети) информации принести прямую финансовую выгоду посторонним лицам?
- Сколько раз за последние 3 года посторонние лица пытались получить несанкционированный доступ к хранящейся в системе (сети) информации иными способами (не пользуясь «маскарадом»)?
- Сколько раз за последние 3 года посторонние лица пытались получить несанкционированный доступ к информации, хранящейся в других подобных системах в вашей организации?
- Где территориально располагается система?

Угроза: **Несанкционированный доступ к приложению**

- Может ли сокрытие информации принести прямую финансовую или иную выгоду сотрудникам?
- Может ли уничтожение информации принести прямую финансовую или иную выгоду сотрудникам?
- Может ли раскрытие информации принести прямую финансовую или иную выгоду сотрудникам?
- Может ли искажение информации принести прямую финансовую или иную выгоду сотрудникам?
- Осведомлен ли персонал о тех выгодах, которые можно получить, воспользовавшись приложением несанкционированным способом?
- Может ли сокрытие какой-либо информации (финансовых счетов, документов политически важного характера) принести существенную выгоду посторонним лицам,

заинтересованным организациям и т. п.?

- Может ли уничтожение какой-либо информации (финансовых счетов, документов политически важного характера) принести существенную выгоду посторонним лицам, заинтересованным организациям и т. п.?
- Может ли раскрытие какой-либо информации (финансовых счетов, документов политически важного характера) принести существенную выгоду посторонним лицам, заинтересованным организациям и т. п.?
- Может ли искажение какой-либо информации (финансовых счетов, документов политически важного характера) принести существенную выгоду посторонним лицам, заинтересованным организациям и т. п.?
- Осведомлены ли упомянутые выше посторонние лица и организации о тех выгодах, которые можно получить, воспользовавшись приложением несанкционированным способом?
- Существуют ли другие, более простые, способы достичь желаемого результата, чем несанкционированное использование приложения?
- Каков общий уровень моральных качеств персонала?
- Каким проверкам подвергается персонал при приеме на работу?
- Известны ли случаи нападения, угроз, шантажа, давления на персонал?
- Является ли обычной практикой использование временно нанятых или работающих по контракту сотрудников для обеспечения нормальной работы информационной системы?
- Подвергался ли кто-нибудь из сотрудников наказаниям или дисциплинарным взысканиям за нарушение нормативных актов, определяющих правила использования компьютеров?
- Сколько случаев несанкционированного использования приложений отмечено за последние 3 года?
- Какова тенденция в статистике попыток несанкционированного использования приложений?

Угроза: **Внедрение вредоносного программного обеспечения**

- Пользуется ли персонал, обслуживающий информационную систему, свободно распространяемым (условно свободно распространяемым – «shareware») или нелегальным программным обеспечением, а также демонстрационными версиями программ; имеют ли сотрудники доступ и получают ли информацию с «досок объявлений» («bulletin boards») или приносят ее на дискетах из дома?
- Получаете ли вы легальное программное обеспечение только от солидных фирм-распространителей?
- Могут ли сервис-инженеры бесконтрольно устанавливать и запускать диагностические программы?
- Используется ли в вашей организации недостаточно отработанное программное обеспечение (т.е. предварительные версии программ)?
- Предусмотрен ли в вашей системе свободный обмен информацией с другими организациями?
- Сколько происшествий, связанных с вредоносным программным обеспечением, произошло за последние 3 года?
- Какова общая тенденция в статистике происшествий, связанных с внедрением вредоносного программного обеспечения в систему?

Угроза: **Злоупотребление системными ресурсами**

- Может ли злоупотребление привлекательными ресурсами (игры, печать на цветных принтерах, доступ к BBS и т.п.) привести к их недоступности в течение 15 минут?
- Может ли злоупотребление привлекательными ресурсами привести к их недоступности в течение 1 часа?
- Может ли злоупотребление программным обеспечением для разработчиков, компиляторами и т.п. привести к его недоступности в течение 15 минут?
- Может ли злоупотребление программным обеспечением для разработчиков, компиляторами и т.п. привести к его

недоступности в течение 1 часа?

- Каков общий уровень моральных качеств персонала?
- Каким проверкам подвергается персонал при приеме на работу?
- Является ли обычной практикой использование временно нанятых или работающих по контракту сотрудников, ответственных за использование ресурсов информационной системы?
- Подвергался ли кто-нибудь из сотрудников наказаниям или дисциплинарным взысканиям за нарушение нормативных актов, определяющих правила использования компьютеров?
- Сколько случаев злоупотребления системными ресурсами отмечено за последние 3 года?

Угроза: **Использование телекоммуникаций для несанкционированного доступа сотрудниками организации**

- Может ли повторная посылка данных принести прямую финансовую или иную выгоду сотрудникам?
- Может ли внеочередная передача данных принести прямую финансовую или иную выгоду сотрудникам?
- Может ли уничтожение данных в процессе их передачи принести прямую финансовую или иную выгоду сотрудникам?
- Может ли добавление лишних данных в процессе их передачи принести прямую финансовую или иную выгоду сотрудникам?
- Может ли искажение данных в процессе их передачи принести прямую финансовую или иную выгоду сотрудникам?
- Может ли недоставка по назначению передаваемых данных принести прямую финансовую или иную выгоду сотрудникам?
- Может ли просмотр и запись данных в процессе их передачи принести прямую финансовую или иную выгоду сотрудникам?
- Может ли знание идентификаторов отправителей и адресатов конкретных сетевых посылок использовано сотрудниками для получения прямых финансовых или иных выгод?
- Может ли маскировка под легитимный хост принести прямую финансовую или иную выгоду сотрудникам?

- Может ли частичный или полный отказ от передачи той или иной информации принести прямую финансовую или иную выгоду сотрудникам?
- Может ли частичный или полный отказ от приема той или иной информации принести прямую финансовую или иную выгоду сотрудникам?
- Осведомлены ли сотрудники о том, что искажение данных в процессе передачи может оказаться для них выгодным?
- Существуют ли другие способы достижения тех же выгод и преимуществ, которые могут оказаться для сотрудников более привлекательными?
- Сколько попыток или реальных случаев несанкционированного внедрения сотрудников в систему с использованием телекоммуникаций и доступа к критическим данным произошло за последние 3 года?
- Сколько попыток или реальных случаев несанкционированного внедрения сотрудников в систему с использованием телекоммуникаций и доступа к прочим данным произошло за последние 3 года?
- Какова общая тенденция в статистике происшествий, связанных с попытками сотрудников получить доступ к данным, передаваемым по коммуникационной сети?
- Подвергался ли кто-нибудь из сотрудников наказаниям или дисциплинарным взысканиям за нарушение нормативных актов, определяющих правила использования компьютеров?
- Был ли предоставлен привилегированный доступ к сети или сетевому оборудованию сотрудникам, предупрежденным о предстоящем увольнении или сокращении?
- Были ли ранее зафиксированы попытки оказать давление на сотрудников?

Угроза: **Использование телекоммуникаций для несанкционированного доступа поставщиком услуг**

- Может ли повторная посылка данных принести прямую финансовую или иную выгоду поставщику услуг?

- Может ли внеочередная передача данных принести прямую финансовую или иную выгоду поставщику услуг?
- Может ли уничтожение данных в процессе их передачи принести прямую финансовую или иную выгоду поставщику услуг?
- Может ли добавление лишних данных в процессе их передачи принести прямую финансовую или иную выгоду поставщику услуг?
- Может ли искажение данных в процессе их передачи принести прямую финансовую или иную выгоду поставщику услуг?
- Может ли недоставка по назначению передаваемых данных принести прямую финансовую или иную выгоду поставщику услуг?
- Может ли просмотр и запись данных в процессе их передачи принести прямую финансовую или иную выгоду поставщику услуг?
- Может ли знание идентификаторов отправителей и адресатов конкретных сетевых посылок использовано поставщиком услуг для получения прямых финансовых или иных выгод?
- Может ли маскировка под легитимный хост принести прямую финансовую или иную выгоду поставщику услуг?
- Осведомлен ли поставщик услуг о том, что искажение данных в процессе передачи может оказаться для него выгодным?
- Существуют ли другие способы достижения тех же выгод и преимуществ, которые могут оказаться для поставщика услуг более привлекательными?
- Сколько попыток или реальных случаев несанкционированного внедрения поставщика услуг в систему с использованием телекоммуникаций и доступа к критическим данным произошло за последние 3 года?
- Сколько попыток или реальных случаев несанкционированного внедрения поставщика услуг в систему с использованием телекоммуникаций и доступа к прочим данным произошло за последние 3 года?
- Подвергался ли кто-нибудь из сотрудников фирмы-

поставщика услуг наказаниям или дисциплинарным взысканиям за нарушение нормативных актов, определяющих правила использования компьютеров?

- Был ли предоставлен привилегированный доступ к сети или сетевому оборудованию сотрудникам фирмы-поставщика услуг, предупрежденным о предстоящем увольнении или сокращении?
- Были ли ранее зафиксированы попытки оказать давление на сотрудников фирмы-поставщика услуг?
- Может ли частичный или полный отказ от передачи той или иной информации принести прямую финансовую или иную выгоду поставщику услуг?
- Может ли частичный или полный отказ от приема той или иной информации принести прямую финансовую или иную выгоду поставщику услуг?
- Какова общая тенденция в статистике происшествий, связанных с попытками поставщиков услуг получить доступ к данным, передаваемым по коммуникационной сети?

Угроза: **Использование телекоммуникаций для несанкционированного доступа посторонними**

- Может ли повторная посылка данных принести прямую финансовую или иную выгоду посторонним лицам?
- Может ли внеочередная передача данных принести прямую финансовую или иную выгоду посторонним лицам?
- Может ли уничтожение данных в процессе их передачи принести прямую финансовую или иную выгоду посторонним лицам?
- Может ли добавление лишних данных в процессе их передачи принести прямую финансовую или иную выгоду посторонним лицам?
- Может ли искажение данных в процессе их передачи принести прямую финансовую или иную выгоду посторонним лицам?
- Может ли недоставка по назначению передаваемых данных

принести прямую финансовую или иную выгоду посторонним лицам?

- Может ли просмотр и запись данных в процессе их передачи принести прямую финансовую или иную выгоду посторонним лицам?
- Может ли знание идентификаторов отправителей и адресатов конкретных сетевых посылок использовано посторонними лицами для получения прямых финансовых или иных выгод?
- Может ли маскировка под легитимный хост принести прямую финансовую или иную выгоду посторонним лицам?
- Осведомлены ли посторонние лица о том, что искажение данных в процессе передачи может оказаться для них выгодным?
- Существуют ли другие способы достижения тех же выгод и преимуществ, которые могут оказаться для посторонних лиц более привлекательными?
- Сколько попыток или реальных случаев несанкционированного внедрения посторонних лиц в систему с использованием телекоммуникаций и доступа к критическим данным произошло за последние 3 года?
- Сколько попыток или реальных случаев несанкционированного внедрения посторонних лиц в систему с использованием телекоммуникаций и доступа к прочим данным произошло за последние 3 года?
- К какой из категорий относятся посторонние лица или организации, которые могут проявить интерес к передаваемым по сети данным?
- Разрешен ли рядовым гражданам физический доступ к сетевым устройствам в обычном режиме работы сети?
- Разрешено ли рядовым гражданам пользоваться сетью в ее обычном режиме работы?
- Используется ли сеть совместно с другими организациями?
- Можно ли получить передаваемую по сети информацию из других источников?
- Какова общая тенденция в статистике происшествий, связанных с попытками посторонних лиц и организаций получить доступ к данным, передаваемым по

коммуникационной сети?

Угроза: **Ошибки при маршрутизации**

- Каков размер сети (количество узлов или адресов)?
- Каково количество маршрутизирующих узлов (таблиц) в сети?
- Каков общий уровень компетенции обслуживающего персонала в вопросах сетевых технологий?
- Сколько случайных ошибок при маршрутизации, зарегистрированных за последние 3 года, имело отношение к критическим данным?
- Сколько случайных ошибок при маршрутизации, зарегистрированных за последние 3 года, имело отношение к другим данным, передававшимся через те же сетевые службы?
- Может ли сложность таблиц маршрутизации или частота внесения в них изменений вызвать беспокойство с точки зрения возрастания вероятности ошибок при маршрутизации данных?
- Может ли сложность таблиц фильтрации или частота внесения в них изменений (в сами таблицы фильтрации или закрытые группы пользователей) вызвать беспокойство с точки зрения возрастания вероятности ошибок при маршрутизации данных?

Угроза: **Неисправность основного компьютера, не включенного в сеть**

- Основной (не сетевой) компьютер выпущен от 1 до 6 лет назад?
- Основной (не сетевой) компьютер – новой конструкции, а значит, еще не прошел всестороннюю проверку и не доказал свою надежность?
- Основной (не сетевой) компьютер подвергался перед установкой специальной доработке?

- Основной (не сетевой) компьютер используется нестандартным образом или выполняет задачи, для которых он не предназначен?
- Нарушаются ли рекомендованные фирмой-изготовителем условия эксплуатации (температура, влажность, запыленность, параметры питающей электросети и т.п.)?
- Основной (не сетевой) компьютер эксплуатируется на пределе своих возможностей?
- Сколько случаев технической неисправности основного (не сетевого) компьютера зафиксировано за последние 3 года?
- Какова общая тенденция в статистике отказов основного (не сетевого) компьютера?

Угроза: **Неисправность сетевого сервера**

- Сетевой сервер выпущен от 1 до 6 лет назад?
- Сетевой сервер – новой конструкции, а значит, еще не прошел всестороннюю проверку и не доказал свою надежность?
- Сетевой сервер подвергался перед установкой специальной доработке?
- Сетевой сервер используется нестандартным образом или выполняет задачи, для которых он не предназначен?
- Нарушаются ли рекомендованные фирмой-изготовителем условия эксплуатации (температура, влажность, запыленность, параметры питающей электросети и т.п.)?
- Сетевой сервер эксплуатируется на пределе своих возможностей?
- Сколько случаев технической неисправности сетевого сервера зафиксировано за последние 3 года?
- Какова общая тенденция в статистике отказов сетевого сервера?

Угроза: **Неисправность накопительного устройства**

- Накопительное устройство выпущено от 1 до 6 лет назад?

- Накопительное устройство – новой конструкции, а значит, еще не прошло всестороннюю проверку и не доказало свою надежность?
- Накопительное устройство подвергалось перед установкой специальной доработке?
- Накопительное устройство используется нестандартным образом или выполняет задачи, для которых оно не предназначено?
- Нарушаются ли рекомендованные фирмой-изготовителем условия эксплуатации (температура, влажность, запыленность, параметры питающей электросети и т.п.)?
- Накопительное устройство эксплуатируется на пределе своих возможностей?
- Сколько случаев технической неисправности накопительного устройства зафиксировано за последние 3 года?
- Какова общая тенденция в статистике отказов накопительного устройства?

Угроза: **Неисправность печатающих устройств**

- Печатающее устройство выпущено от 1 до 6 лет назад?
- Печатающее устройство – новой конструкции, а значит, еще не прошло всестороннюю проверку и не доказало свою надежность?
- Печатающее устройство подвергалось перед установкой специальной доработке?
- Печатающее устройство используется нестандартным образом или выполняет задачи, для которых оно не предназначено?
- Нарушаются ли рекомендованные фирмой-изготовителем условия эксплуатации (температура, влажность, запыленность, параметры питающей электросети и т.п.)?
- Печатающее устройство эксплуатируется на пределе своих возможностей?
- Сколько случаев технической неисправности печатающего устройства зафиксировано за последние 3 года?
- Какова общая тенденция в статистике отказов печатающего

устройства?

Угроза: **Неисправность сетевых распределяющих компонентов**

- Сетевой распределяющий компонент выпущен от 1 до 6 лет назад?
- Сетевой распределяющий компонент новой конструкции, а, значит, еще не прошел всестороннюю проверку и не доказал свою надежность?
- Сетевой распределяющий компонент подвергался перед установкой специальной доработке?
- Сетевой распределяющий компонент используется нестандартным образом или выполняет задачи, для которых он не предназначен?
- Нарушаются ли рекомендованные фирмой-изготовителем условия эксплуатации (температура, влажность, запыленность, параметры питающей электросети и т.п.)?
- Сетевой распределяющий компонент эксплуатируется на пределе своих возможностей?
- Сколько случаев технической неисправности сетевого распределяющего компонента зафиксировано за последние 3 года?
- Какова общая тенденция в статистике отказов сетевого распределяющего компонента?

Угроза: **Неисправность сетевых шлюзов**

- Сетевой шлюз выпущен от 1 до 6 лет назад?
- Сетевой шлюз – новой конструкции, а значит, еще не прошел всестороннюю проверку и не доказал свою надежность?
- Сетевой шлюз подвергался перед установкой специальной доработке?
- Сетевой шлюз используется нестандартным образом или выполняет задачи, для которых он не предназначен?
- Нарушаются ли рекомендованные фирмой-изготовителем

условия эксплуатации (температура, влажность, запыленность, параметры питающей электросети и т.п.)?
- Сетевой шлюз эксплуатируется на пределе своих возможностей?
- Сколько случаев технической неисправности сетевого шлюза зафиксировано за последние 3 года?
- Какова общая тенденция в статистике отказов сетевого шлюза?

Угроза: **Неисправность средств сетевого управления или управляющих серверов**

- Средство сетевого управления или управляющий сервер выпущен от 1 до 6 лет назад?
- Средство сетевого управления или управляющий сервер – новой конструкции, а значит, еще не прошел всестороннюю проверку и не доказал свою надежность?
- Средство сетевого управления или управляющий сервер подвергался перед установкой специальной доработке?
- Средство сетевого управления или управляющий сервер используется нестандартным образом или выполняет задачи, для которых он не предназначен?
- Нарушаются ли рекомендованные фирмой-изготовителем условия эксплуатации (температура, влажность, запыленность, параметры питающей электросети и т.п.)?
- Средство сетевого управления или управляющий сервер эксплуатируется на пределе своих возможностей?
- Сколько случаев технической неисправности средства сетевого управления или управляющего сервера зафиксировано за последние 3 года?
- Какова общая тенденция в статистике отказов средства сетевого управления или управляющего сервера?

Угроза: **Неисправность сетевых интерфейсов**

- Часто ли перекоммутируются кабели, распределительные и

нагрузочные устройства, имеющие непосредственное отношение к передаче данных?
- Располагаются ли кабели, распределительные и нагрузочные устройства в зонах с повышенным уровнем электромагнитных помех?
- Располагаются ли кабели, распределительные и нагрузочные устройства в зонах с повышенным риском случайного повреждения, например в результате ремонта?
- Сколько раз за последние 3 года работа системы прерывалась более чем на час из-за неполадок в сетевых интерфейсах?

Угроза: **Неисправность сетевых сервисов**

- Предусмотрен ли сетевой сервис в соответствии с общепринятыми уровнями?
- Сколько раз за последние 3 года работа системы прерывалась более чем на час из-за неисправности сетевого сервиса?
- Какова общая тенденция в статистике неисправностей сетевого сервиса?

Угроза: **Неисправность электропитания**

- Сколько раз за последние 3 года штатные источники электропитания отключались более чем на 3 часа?
- Сколько раз за последние 3 года штатные источники электропитания отключались более чем на 1 час, но менее чем на 3 часа?
- Сколько раз за последние 3 года штатные источники электропитания отключались более чем на 15 минут, но менее чем на 1 час?
- Какова общая тенденция в статистике отказов источников электропитания?
- Располагается ли система или ее отдельные компоненты в непосредственной близости от зон с повышенным риском

аварий питающей электросети?

Угроза: **Неисправность кондиционеров**

- Система установлена в стране, где температура воздуха регулярно повышается до 40 °C и более?
- Кондиционеры выпущены от 1 до 6 лет назад?
- Кондиционеры – новой конструкции, а значит, еще не прошли всестороннюю проверку и не доказали свою надежность?
- Кондиционеры подвергались перед установкой специальной доработке?
- Кондиционеры эксплуатируются на пределе своих возможностей?
- Сколько раз за последние 3 года кондиционеры выходили из строя?
- Какова общая тенденция в статистике отказов кондиционеров?

Угроза: **Сбои системного и сетевого ПО**

- Сколько раз за последние 3 года работа прерывалась более чем на 12 часов из-за сбоев системного или сетевого ПО?
- Сколько раз за последние 3 года работа прерывалась более чем на 3 часа, но менее чем на 12 часов из-за сбоев системного или сетевого ПО?
- Сколько раз за последние 3 года работа прерывалась более чем на 1 час, но менее чем на 3 часа из-за сбоев системного или сетевого ПО?
- Сколько раз за последние 3 года работа прерывалась более чем на 15 минут, но менее чем на 1 час из-за сбоев системного или сетевого ПО?
- Сколько раз за последние 3 года из-за сбоев системного или сетевого ПО происходила утечка информации?
- Сколько раз за последние 3 года из-за сбоев системного или сетевого ПО происходило незначительное

несанкционированное искажение информации?

- Сколько раз за последние 3 года из-за сбоев системного или сетевого ПО происходило обширное несанкционированное искажение информации?
- Как выглядит «послужной список» фирмы-разработчика вашего системного и сетевого ПО?
- Системное и сетевое ПО разработано недавно или построено на новых принципах, а значит, еще не прошло всестороннюю проверку и не доказало свою надежность?
- Системное и сетевое ПО подвергалось перед установкой специальной доработке?
- Какова общая тенденция в статистике сбоев системного и сетевого ПО?

Угроза: **Сбои прикладного ПО**

- Сколько раз за последние 3 года работа прерывалась более чем на 12 часов из-за сбоев прикладного ПО?
- Сколько раз за последние 3 года работа прерывалась более чем на 3 часа, но менее чем на 12 часов из-за сбоев прикладного ПО?
- Сколько раз за последние 3 года работа прерывалась более чем на 1 час, но менее чем на 3 часа из-за сбоев прикладного ПО?
- Сколько раз за последние 3 года работа прерывалась более чем на 15 минут, но менее чем на 1 час из-за сбоев прикладного ПО?
- Сколько раз за последние 3 года работа прерывалась менее чем на 15 минут из-за сбоев прикладного ПО?
- Сколько раз за последние 3 года из-за сбоев прикладного ПО информация становилась доступной лицам, не обладающим соответствующими правами, или обслуживающему персоналу?
- Сколько раз за последние 3 года из-за сбоев прикладного ПО происходило незначительное несанкционированное искажение информации?
- Сколько раз за последние 3 года из-за сбоев прикладного

ПО происходило обширное несанкционированное искажение информации?
- Не перегружены ли программисты работой настолько, что это может повысить риск возникновения ошибки?
- На каком языке пишутся программы?
- Каков профессиональный опыт прикладных программистов, разрабатывающих ПО данного конкретного типа?
- Какова общая тенденция в статистике сбоев прикладного ПО?

Угроза: **Ошибки операторов**

- Сколько раз за последние 3 года ошибки операторов приводили к потере работоспособности системы?
- Сколько раз за последние 3 года ошибки операторов приводили к утечке информации?
- Сколько раз за последние 3 года ошибки операторов приводили к искажениям данных?
- Сколько операторов обслуживают основную систему?
- Не перегружены ли операторы работой настолько, что это может повысить риск возникновения ошибки?
- Каков профессиональный опыт операторов (в среднем)?
- Какова общая тенденция в статистике операторских ошибок?

Угроза: **Ошибки при профилактических работах с оборудованием**

- Сколько раз за последние 3 года ошибки при профилактических работах с оборудованием приводили к потере работоспособности системы?
- Сколько раз за последние 3 года ошибки при профилактических работах с оборудованием приводили к утечке информации?
- Существовали ли ранее претензии к качеству выполнения профилактических работ с оборудованием?
- Сколько человек занимаются профилактикой оборудования?
- Не перегружены ли сотрудники, выполняющие

профилактические работы с оборудованием, настолько, что это может повысить риск возникновения ошибки?
- Каков профессиональный опыт сотрудников, выполняющих профилактические работы с оборудованием (в среднем)?

Угроза: **Ошибки при профилактических работах с ПО**

- Сколько раз за последние 3 года персонал, выполняющий профилактические работы с ПО, допускал ошибки, приводившие к потере работоспособности системы?
- Сколько раз за последние 3 года персонал, выполняющий профилактические работы с ПО, допускал ошибки, приводившие к утечке информации?
- Сколько раз за последние 3 года персонал, выполняющий профилактические работы с ПО, допускал ошибки, приводившие к искажению данных?
- Сколько человек занимаются профилактикой ПО на основной системе?
- Не перегружены ли сотрудники, выполняющие профилактические работы с ПО, настолько, что это может повысить риск возникновения ошибки?
- Каков профессиональный опыт сотрудников, выполняющих профилактические работы с ПО (в среднем)?

Угроза: **Ошибки пользователей**

- Сколько раз за последние 3 года ошибки пользователей приводили к потере работоспособности системы?
- Сколько раз за последние 3 года ошибки пользователей приводили к утечке информации?
- Сколько раз за последние 3 года ошибки пользователей приводили к незначительным искажениям данных?
- Сколько пользователей работает с приложением?
- Не перегружены ли пользователи настолько, что это может повысить риск возникновения ошибки?
- Каков опыт пользователей в их сфере деятельности (в

среднем)?

- Каков опыт пользователей в работе с конкретным приложением (в среднем)?
- Какую долю операций, выполняемых при работе с конкретным приложением, можно отнести к категории элементарных (например, обычные операции копирования)?
- Какую долю операций, выполняемых при работе с конкретным приложением, можно отнести к категории действий средней сложности (например, операции, требующие проведения вычислений или ввода данных, за которыми нужно обращаться к справочникам)?
- Какую долю операций, выполняемых при работе с конкретным приложением, можно отнести к категории сложных (например, требующих создания новых документов)?
- Какова общая тенденция в статистике ошибок пользователей?

Угроза: **Пожар**

- Сколько пожаров или возгораний любой степени тяжести произошло за последние 3 года?
- Располагаются ли поблизости от системы устройства, относящиеся к категории пожароопасных (например, электроплитки)?
- Разрешено ли курить в непосредственной близости от ответственных компонентов оборудования информационной системы?
- Располагаются ли поблизости от системы экспериментальные или нестандартные устройства, представляющие опасность с точки зрения возможного возгорания в результате короткого замыкания (например, оборудование, находящееся на стадии разработки, силовые коммутационные устройства, старая электропроводка и т.п.)?
- Представляют ли опасность с точки зрения распространения пожара соседние здания или помещения в том же здании, но занимаемые другими организациями (например, не хранятся

ли в них запасы бумаги для принтеров, не расположены ли рядом бензозаправочные станции и т.п.)?
- Установлены ли поблизости баки с горючим, не оборудованные в соответствии с правилами пожарной безопасности?
- Достаточно ли в помещении (здании) точек подключения к силовой электросети всех устройств, необходимых для нормальной работы (в первую очередь оцените, не перегружены ли электрические розетки)?
- Какова общая тенденция в статистике пожаров?

Угроза: **Затопление**

- Сколько случаев затопления произошло за последние 3 года?
- Какова общая тенденция в статистике затоплений?
- Проходят ли трубы, по которым протекает вода, через или над помещением, где располагаются ответственные компоненты информационной системы (речь идет о трубах центрального отопления, водопроводных или относящихся к общей системе кондиционирования здания)?
- Располагаются ли поблизости резервуары, вода из которых в случае утечки может нанести ущерб ответственным компонентам информационной системы?
- Возможны ли иные аварийные ситуации в здании, при которых будут затоплены ответственные компоненты информационной системы (например, протечка плоской крыши при ливне, неисправность пожарного гидранта и т.п.)
- Может ли наводнение в результате выхода из берегов близлежащей реки или водохранилища нанести ущерб ответственным компонентам информационной системы?

Угроза: **Природные катаклизмы**

- Может ли здание пострадать в результате воздействия природных катаклизмов?

- Сколько случаев нарушения работы вычислительного комплекса в результате природных катаклизмов было зафиксировано за последние 3 года?
- Какова общая тенденция в статистике природных катаклизмов?

Угроза: **Нехватка персонала**

- Сколько раз за последние 3 года нарушалась работа информационной системы по причинам, не связанным с забастовками (речь идет о болезнях сотрудников, проблемах с транспортом, эвакуации персонала и т.п.)?
- Сколько раз за последние 3 года нарушалась работа информационной системы по причинам, связанным с забастовками?
- Каков общий уровень моральных качеств персонала?
- Какова общая тенденция в статистике нарушений работы информационной системы по причинам, связанным с нехваткой персонала?

Угроза: **Кражи со стороны сотрудников**

- Сколько случаев краж со стороны сотрудников зафиксировано за последние 3 года?
- Что крали (если есть несколько вариантов ответов, выберите один из них с максимальным количеством баллов)?
- Кем кражи производились?
- Понимают ли сотрудники, какую выгоду они могут получить в результате кражи оборудования?
- Подвергался ли кто-нибудь из сотрудников наказаниям или дисциплинарным взысканиям за нарушение законодательных актов, связанных с защитой данных, авторских прав и т.п.?
- Были ли ранее зафиксированы попытки оказать давление на кого-либо из сотрудников?
- Каков общий уровень моральных качеств персонала?

- Понимают ли сотрудники, какую выгоду они могут получить в результате кражи информации?

Угроза: **Кражи со стороны посторонних**

- Сколько случаев краж со стороны посторонних зафиксировано за последние 3 года?
- Что крали (если есть несколько вариантов ответов, выберите один из них с максимальным количеством баллов)?
- кражи производились:
- Понимают ли посторонние лица, какую выгоду они могут получить в результате кражи оборудования?
- Сколько посетителей входит в здание за день (в среднем)?
- Понимают ли посторонние лица, какую выгоду они могут получить в результате кражи информации?

Угроза: **Преднамеренное вредительство со стороны сотрудников**

- Сколько человек имеют доступ в помещение или зону размещения системы?
- Существуют ли группы сотрудников или отдельные личности, моральные качества которых невысоки?
- Сколько случаев преднамеренного вредительства со стороны сотрудников зафиксировано за последние 3 года?
- Какова общая тенденция в статистике случаев преднамеренного вредительства со стороны сотрудников?
- Может ли сотрудник получить финансовую выгоду в результате преднамеренного вредительства?
- Сколько человек имеют доступ в здание?

Угроза: **Преднамеренное вредительство со стороны посторонних**

- Располагается ли система на территории, где часто совершаются акты вандализма?
- Сколько раз за последние 3 года посторонними лицами

наносился ущерб зданию?

- Какова общая тенденция в статистике случаев преднамеренного вредительства со стороны посторонних?
- Какая из нижеперечисленных групп может быть заинтересована в причинении физического ущерба зданию?

Угроза: **Терроризм**

- Осведомлены ли экстремистские и террористические группировки о тех выгодах, которые они могут получить в результате нападения на организацию? Расположено ли здание во враждебном окружении или рядом с потенциальной мишенью террористов?
- Имеются ли данные о том, что определенные группировки совершали нападения?
- Какова ощутимая тенденция в статистике нападений определенных группировок?
- Получала ли организация заслуживающие доверия предупреждения о возможных нападениях со стороны экстремистских или террористических группировок? Не пытались ли подобные группировки вступить в контакт с кем-либо из сотрудников?
- Имеют ли определенные группировки возможность совершить нападение?
- Располагают ли определенные группировки необходимыми для нападения ресурсами?