Приложение 8. Опросный лист для оценки уязвимостей по методу CRAMM

написано Александр Астахов | 11 июня, 2023

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

- Сколько человек имеют право пользоваться системой (сетью)?
- Будет ли линейное руководство осведомлено о том, что люди, работающие под их началом, ведут себя необычным образом?
- Какие устройства и программы доступны пользователям?
- Возможны ли ситуации, когда сотрудникам, предупрежденным о предстоящем сокращении или увольнении, разрешается логический доступ к системе (сети)?
- Каковы в среднем размеры рабочих групп сотрудников пользовательских подразделений, имеющих доступ к системе (сети)?
- Станет ли факт изменения хранящихся в системе (сети) данных очевидным сразу для нескольких человек (в результате чего его будет очень трудно скрыть)?
- Насколько велики официально предоставленные пользователям возможности по просмотру всех хранящихся в системе данных?
- Насколько необходимо пользователям знать всю информацию, хранящуюся в системе?

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

- Какое количество учетных записей пользователей хранится в системе (сети)?

- Будут ли сотрудники организации осведомлены о том, что люди, работающие у поставщика услуг, ведут себя необычным образом?
- Какие устройства и программы доступны поставщикам услуг?
- Возможны ли ситуации, когда сотрудникам организации-поставщика услуг, предупрежденным о предстоящем сокращении или увольнении, разрешается логический доступ к системе (сети)?
- Входит ли в обязанности кого-либо из сотрудников организации-поставщика услуг программирование приложений для системы?
- Станет ли факт изменения хранящихся в системе (сети) данных очевидным сразу для нескольких человек (в результате чего его будет очень трудно скрыть)?

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

- Какое количество учетных записей пользователей хранится в системе (сети)?
- Разрешено ли пользоваться системой (сетью) рядовым гражданам?
- К какой внешней сети подключена рассматриваемая система (сеть)?
- Насколько велики официально предоставленные пользователям возможности по просмотру всех хранящихся в системе данных?
- Насколько необходимо пользователям знать всю информацию, хранящуюся в системе?

Угроза: **Несанкционированный доступ к приложению**

- Обладают ли сотрудники достаточными знаниями и возможностями для того, чтобы использовать приложение несанкционированным образом (например, обойти блокировки и получить непосредственный доступ к данным)?

- Каков общий уровень загруженности персонала, имеющего доступ к приложениям?
- Есть ли у сотрудников возможность использовать приложение несанкционированным образом (например, когда их непосредственно не контролируют, по вечерам и т.п.)?
- Есть ли у сотрудников основания полагать, что использование ими приложения несанкционированным образом останется незамеченным?
- Могут ли сотрудники без официального предупреждения (разрешения) получить физический или логический доступ к критичным с точки зрения функционирования информационной системы программам и устройствам?
- Как скажется на пользователях недоступность приложения?
- Может ли использование приложения несанкционированным образом привести к разрушению информации?
- Может ли использование приложения несанкционированным образом привести к разглашению информации?
- Может ли использование приложения несанкционированным образом привести к искажению информации?

Угроза: **Внедрение вредоносного программного обеспечения**

- Могут ли сотрудники инсталлировать и запускать неразрешенное программное обеспечение (в том числе и с помощью электронной почты)?
- Существуют ли ограничения на использование дискет (например, запрет на считывание с них информации)?
- Если вредоносный программный код все же занесен в одну из частей системы, может ли он воспроизвести сам себя и оказать влияние на работу?
- Как скажется на других пользователях внедрение вредоносного программного обеспечения?
- Может ли внедрение вредоносного программного обеспечения привести к разрушению информации?
- Может ли внедрение вредоносного программного обеспечения привести к разглашению информации?

- Может ли внедрение вредоносного программного обеспечения привести к искажению информации?

Угроза: **Злоупотребление системными ресурсами**

- Обладают ли сотрудники достаточными знаниями и возможностями для того, чтобы извлечь выгоду из использования привлекательных для них устройств и программ?
- Каков общий уровень загруженности персонала?
- Есть ли у сотрудников возможность злоупотребления системными ресурсами (например, над ними не установлен жесткий контроль, соответствующие устройства не располагаются в изолированных зонах)?
- Есть ли у сотрудников основания полагать, что злоупотребления системными ресурсами останутся незамеченными?
- Могут ли сотрудники без официального предупреждения (разрешения) получить физический или логический доступ к критичным с точки зрения функционирования информационной системы программам и устройствам?
- Как скажется на пользователях злоупотребление системными ресурсами? Ресурсы, критичные с точки зрения злоупотребления ими, перечислены в анкете, посвященной угрозам.

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

- Входят ли в состав сети линии связи, проходящие вне территории, находящейся под непосредственным контролем организации?
- Входят ли в состав сети радиочастотные, микроволновые или иные беспроводные линии связи?
- Могут ли сотрудники получить доступ к внутренним линиям связи или сетевому оборудованию на время, достаточное

для того, чтобы осуществить несанкционированный доступ к системе?

- Могут ли сотрудники узнать, по каким каналам передаются данные?
- Обладают ли сотрудники техническими познаниями и доступно ли им программное обеспечение и оборудование, необходимое для изменения сетевого трафика?
- Передаются ли данные в таком формате, что их характер и конкретные значения могут быть распознаны сотрудниками?
- Носят ли данные такой характер, что их искажения могут быть легко обнаружены санкционированными пользователями?
- Легко ли сотрудникам получить в свое распоряжение оборудование, необходимое для перехвата и изменения сетевого трафика (например, сетевые анализаторы, модули маршрутизации, спутниковые широкополосные демодуляторы)?
- Если сфера действия сети распространяется на большую территорию, то выполняется ли маршрутизация так, что данные обычно передаются по одним и тем же каналам (например, по выделенным линиям)?
- Замечаются и расследуются ли руководством и персоналом случаи необычной деятельности в сети?
- Доступна ли другая информация, с помощью которой можно было бы подтвердить подлинность исходных данных?
- Построена ли сеть таким образом, что сотрудникам было бы затруднительно подключить аппаратуру для перехвата и записи данных (например, в сети широко используются оптоволоконные кабели)?
- Строятся ли отношения между отправителями и получателями передаваемой через сеть информации в основном на доверии (т.е. не являются формальными контрактными коммерческими связями)?
- Знакомы ли между собой лично отправители и получатели передаваемой через сеть информации, связаны ли они длительными деловыми отношениями?
- Построена ли система прикладных программ или сетевая служба таким образом, что получатель в состоянии каким-либо дополнительным способом проверить достоверность

принятых сообщений?

- Существуют ли другие отправители аналогичных данных, от которых можно было бы получить какие-либо подтверждения достоверности источника информации?

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

- Входят ли в состав сети линии связи, проходящие вне территории, находящейся под непосредственным контролем организации?
- Входят ли в состав сети радиочастотные, микроволновые или иные беспроводные линии связи?
- Могут ли поставщики услуг получить доступ к внутренним линиям связи или сетевому оборудованию на время, достаточное для того, чтобы осуществить несанкционированный доступ к системе?
- Могут ли поставщики услуг узнать, по каким каналам передаются данные?
- Обладают ли поставщики услуг техническими познаниями и доступно ли им программное обеспечение и оборудование, необходимое для изменения сетевого трафика (например, выдачи ответов, внеочередной пересылки, ввода, искажения или невыдачи данных)?
- Передаются ли данные в таком формате, что их характер и конкретные значения могут быть распознаны поставщиками услуг?
- Носят ли данные такой характер, что их искажения могут быть легко обнаружены санкционированными пользователями?
- Легко ли поставщикам услуг получить в свое распоряжение оборудование, необходимое для перехвата и изменения сетевого трафика (например, сетевые анализаторы, модули маршрутизации, спутниковые широкополосные демодуляторы)?
- Если сфера действия сети распространяется на большую территорию, то выполняется ли маршрутизация так, что данные обычно передаются по одним и тем же каналам

(например, по выделенным линиям)?

- Замечаются и расследуются ли руководством и персоналом случаи необычной деятельности в сети?
- Доступна ли другая информация, с помощью которой можно было бы подтвердить подлинность исходных данных?
- Построена ли сеть таким образом, что поставщикам услуг было бы затруднительно подключить аппаратуру для перехвата и записи данных (например, в сети широко используются оптоволоконные кабели)?

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

- Входят ли в состав сети линии связи, проходящие вне территории, находящейся под непосредственным контролем организации?
- Входят ли в состав сети радиочастотные, микроволновые или иные беспроводные линии связи?
- Могут ли посторонние лица получить доступ к внутренним линиям связи или сетевому оборудованию на время, достаточное для того, чтобы осуществить несанкционированный доступ к системе?
- Могут ли посторонние лица узнать, по каким каналам передаются данные?
- Обладают ли посторонние лица техническими познаниями и доступно ли им программное обеспечение и оборудование, необходимое для изменения сетевого трафика (например, выдачи ответов, внеочередной пересылки, ввода, искажения или невыдачи данных)?
- Передаются ли данные в таком формате, что их характер и конкретные значения могут быть распознаны посторонними лицами?
- Носят ли данные такой характер, что их искажения могут быть легко обнаружены санкционированными пользователями?
- Легко ли посторонним лицам получить в свое распоряжение оборудование, необходимое для перехвата и изменения

сетевого трафика (например, сетевые анализаторы, модули маршрутизации, спутниковые широкополосные демодуляторы)?
- Если сфера действия сети распространяется на большую территорию, то выполняется ли маршрутизация так, что данные обычно передаются по одним и тем же каналам (например, по выделенным линиям)?
- Замечаются и расследуются ли руководством и персоналом случаи необычной деятельности в сети?
- Доступна ли другая информация, с помощью которой можно было бы подтвердить подлинность исходных данных?
- Построена ли сеть таким образом, что поставщикам услуг было бы затруднительно подключить аппаратуру для перехвата и записи данных (например, в сети широко используются оптоволоконные кабели)?

Угроза: **Ошибки при маршрутизации**

- Используется ли в сети много коммуникационных протоколов и схем адресации?
- Осуществляется ли маршрутизация и адресация в сети централизованно (т.е. с помощью сетевой службы управления или ее аналога) с обязательной регистрацией событий и аварийных предупреждений?
- Используется ли в сети строго упорядоченная схема адресации и именования узлов?
- Построены ли приложения или сетевая служба управления таким образом, что ошибочная доставка данных или их части может быть обнаружена санкционированными пользователями или с помощью технических приемов?

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

- Может ли неисправность единственного компонента привести к прекращению обслуживания всех пользователей?
- Возможно ли переконфигурировать систему так, чтобы

обойти неисправность основного (не сетевого) компьютера и избежать вышеупомянутого эффекта?

- Возможна ли доставка необходимых для ремонта материалов и оборудования в короткие сроки, с тем чтобы можно было избежать вышеупомянутого эффекта, т.е. оговорено ли, например, такое условие в контракте на обслуживание?
- Возможно ли устранить неисправность основного (не сетевого) компьютера в течение 15 минут?
- Возможно ли устранить неисправность основного (не сетевого) компьютера в течение одного часа?
- Возможно ли устранить неисправность основного (не сетевого) компьютера в течение 3 часов?
- Возможно ли устранить неисправность основного (не сетевого) компьютера в течение 12 часов?
- Возможно ли устранить неисправность основного (не сетевого) компьютера в течение одного дня?
- Возможно ли устранить неисправность основного (не сетевого) компьютера в течение 2 дней?

Угроза: **Неисправность сетевого сервера**

- Может ли неисправность единственного компонента привести к прекращению обслуживания всех пользователей?
- Возможно ли переконфигурировать систему так, чтобы обойти неисправность сетевого сервера и избежать вышеупомянутого эффекта?
- Возможна ли доставка необходимых для ремонта материалов и оборудования в короткие сроки, с тем чтобы можно было избежать вышеупомянутого эффекта, т.е. оговорено ли, например, такое условие в контракте на обслуживание?
- Возможно ли устранить неисправность сетевого сервера в течение 15 минут?
- Возможно ли устранить неисправность сетевого сервера в течение одного часа?
- Возможно ли устранить неисправность сетевого сервера в течение 3 часов?

- Возможно ли устранить неисправность сетевого сервера в течение 12 часов?
- Возможно ли устранить неисправность сетевого сервера в течение одного дня?
- Возможно ли устранить неисправность сетевого сервера в течение 2 дней?

Угроза: **Неисправность накопительного устройства**

- Может ли неисправность единственного компонента привести к прекращению обслуживания всех пользователей?
- Возможно ли переконфигурировать систему так, чтобы обойти неисправность накопительного устройства и избежать вышеупомянутого эффекта?
- Возможна ли доставка необходимых для ремонта материалов и оборудования в короткие сроки, с тем чтобы можно было избежать вышеупомянутого эффекта, т.е. оговорено ли, например, такое условие в контракте на обслуживание?
- Возможно ли устранить неисправность накопительного устройства в течение 15 минут?
- Возможно ли устранить неисправность накопительного устройства в течение одного часа?
- Возможно ли устранить неисправность накопительного устройства в течение 3 часов?
- Возможно ли устранить неисправность накопительного устройства в течение 12 часов?
- Возможно ли устранить неисправность накопительного устройства в течение одного дня?
- Возможно ли устранить неисправность накопительного устройства в течение 2 дней?

Угроза: **Неисправность печатающих устройств**

- Может ли неисправность единственного компонента привести к прекращению обслуживания всех пользователей?
- Возможно ли переконфигурировать систему так, чтобы

обойти неисправность печатающего устройства и избежать вышеупомянутого эффекта?

- Возможна ли доставка необходимых для ремонта материалов и оборудования в короткие сроки, с тем чтобы можно было избежать вышеупомянутого эффекта, т.е. оговорено ли, например, такое условие в контракте на обслуживание?
- Возможно ли устранить неисправность печатающего устройства в течение 15 минут?
- Возможно ли устранить неисправность печатающего устройства в течение одного часа?
- Возможно ли устранить неисправность печатающего устройства в течение 3 часов?
- Возможно ли устранить неисправность печатающего устройства в течение 12 часов?

Угроза: **Неисправность сетевых распределяющих компонентов**

- Может ли неисправность единственного компонента привести к прекращению обслуживания всех пользователей?
- Возможно ли переконфигурировать систему так, чтобы обойти неисправность сетевого распределяющего компонента и избежать вышеупомянутого эффекта?
- Возможна ли доставка необходимых для ремонта материалов и оборудования в короткие сроки, с тем чтобы можно было избежать вышеупомянутого эффекта, т.е. оговорено ли, например, такое условие в контракте на обслуживание?
- Возможно ли устранить неисправность сетевого распределяющего компонента в течение 15 минут?
- Возможно ли устранить неисправность сетевого распределяющего компонента в течение одного часа?
- Возможно ли устранить неисправность сетевого распределяющего компонента в течение 3 часов?
- Возможно ли устранить неисправность сетевого распределяющего компонента в течение 12 часов?
- Возможно ли устранить неисправность сетевого распределяющего компонента в течение одного дня?

- Возможно ли устранить неисправность сетевого распределяющего компонента в течение 2 дней?

Угроза: **Неисправность сетевых шлюзов**

- Может ли неисправность единственного компонента привести к прекращению обслуживания всех пользователей?
- Возможно ли переконфигурировать систему так, чтобы обойти неисправность сетевого шлюза и избежать вышеупомянутого эффекта?
- Возможна ли доставка необходимых для ремонта материалов и оборудования в короткие сроки, с тем чтобы можно было избежать вышеупомянутого эффекта, т.е. оговорено ли, например, такое условие в контракте на обслуживание?
- Возможно ли устранить неисправность сетевого шлюза в течение 15 минут?
- Возможно ли устранить неисправность сетевого шлюза в течение одного часа?
- Возможно ли устранить неисправность сетевого шлюза в течение 3 часов?
- Возможно ли устранить неисправность сетевого шлюза в течение 12 часов?
- Возможно ли устранить неисправность сетевого шлюза в течение одного дня?
- Возможно ли устранить неисправность сетевого шлюза в течение 2 дней?

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

- Может ли неисправность единственного компонента привести к прекращению обслуживания всех пользователей?
- Возможно ли переконфигурировать систему так, чтобы обойти неисправность средства сетевого управления или управляющего сервера и избежать вышеупомянутого эффекта?
- Возможна ли доставка необходимых для ремонта материалов

и оборудования в короткие сроки, с тем чтобы можно было избежать вышеупомянутого эффекта, т.е. оговорено ли, например, такое условие в контракте на обслуживание?

- Возможно ли устранить неисправность средства сетевого управления или управляющего сервера в течение 15 минут?
- Возможно ли устранить неисправность средства сетевого управления или управляющего сервера в течение одного часа?
- Возможно ли устранить неисправность средства сетевого управления или управляющего сервера в течение 3 часов?
- Возможно ли устранить неисправность средства сетевого управления или управляющего сервера в течение 12 часов?
- Возможно ли устранить неисправность средства сетевого управления или управляющего сервера в течение одного дня?
- Возможно ли устранить неисправность средства сетевого управления или управляющего сервера в течение 2 дней?

Угроза: **Неисправность сетевых интерфейсов**

- Переделывались ли сетевые интерфейсы тем или иным способом, в результате чего они стали нестандартными?
- Включено ли обслуживание сетевых интерфейсов в сервисный контракт?
- Составляются ли при неисправностях отчеты с подробной диагностикой повреждений?
- Возможно ли устранить неисправность сетевых интерфейсов в течение 15 минут?
- Возможно ли устранить неисправность сетевых интерфейсов в течение одного часа?
- Возможно ли устранить неисправность сетевых интерфейсов в течение 3 часов?
- Возможно ли устранить неисправность сетевых интерфейсов в течение 12 часов?

Угроза: **Неисправность сетевых сервисов**

- Как скажется на пользователях неисправность сетевых сервисов?

Угроза: **Неисправность электропитания**

- Может ли электропитание быть восстановлено при обычных обстоятельствах в течение 3 часов?
- Может ли электропитание быть восстановлено при обычных обстоятельствах в течение одного часа?
- Может ли электропитание быть восстановлено при обычных обстоятельствах в течение 15 минут?

Угроза: **Неисправность кондиционеров**

- Будет ли прекращена работа информационной системы при неисправности одного единственного кондиционера?
- Может ли кондиционер быть отремонтирован при обычных обстоятельствах в течение одного дня?
- Может ли кондиционер быть отремонтирован при обычных обстоятельствах в течение 12 часов?
- Может ли кондиционер быть отремонтирован при обычных обстоятельствах в течение 3 часов?
- Может ли кондиционер быть отремонтирован при обычных обстоятельствах в течение одного часа?
- Может ли кондиционер быть отремонтирован при обычных обстоятельствах в течение 15 минут?

Угроза: **Сбои системного и сетевого ПО**

- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение 3 часов после сбоя системного или сетевого ПО?
- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение одного часа после сбоя системного или сетевого ПО?

- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение 15 минут после сбоя системного или сетевого ПО?
- Может ли сбой системного или сетевого ПО привести к утечке информации к посторонним лицам?
- Может ли сбой системного или сетевого ПО привести к утечке информации к поставщикам услуг?
- Может ли сбой системного или сетевого ПО привести к утечке информации к сотрудникам?
- Может ли сбой системного или сетевого ПО привести к незначительному искажению информации?
- Может ли сбой системного или сетевого ПО привести к обширному искажению информации?
- Можно ли обнаружить ошибки в данных?
- Поддерживается ли в настоящее время версия установленного системного или сетевого ПО?

Угроза: **Сбои прикладного ПО**

- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение 3 часов после сбоя прикладного ПО?
- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение одного часа после сбоя прикладного ПО?
- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение 15 минут после сбоя прикладного ПО?
- Может ли сбой прикладного ПО привести к утечке информации к сотрудникам, не имеющим допуска к ней?
- Может ли сбой прикладного ПО привести к незначительному искажению информации?
- Может ли сбой прикладного ПО привести к обширному искажению информации?
- Можно ли обнаружить ошибки в данных?
- Насколько серьезно скажется на деятельности организации

прекращение работы системы на срок до 12 часов?

Угроза: **Ошибки операторов**

- Может ли работоспособность информационной системы быть восстановлена при обычных обстоятельствах в течение 3 часов после ошибки оператора?
- Может ли работоспособность информационной системы быть восстановлена при обычных обстоятельствах в течение одного часа после ошибки оператора?
- Может ли работоспособность информационной системы быть восстановлена при обычных обстоятельствах в течение 15 минут после ошибки оператора?
- Может ли ошибка оператора привести к утечке информации к посторонним лицам?
- Может ли ошибка оператора привести к утечке информации к поставщикам услуг?
- Может ли ошибка оператора привести к утечке информации к сотрудникам?
- Может ли ошибка оператора привести к незначительному искажению информации?
- Может ли ошибка оператора привести к обширному искажению информации?
- Можно ли обнаружить ошибки в данных?

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

- Может ли работоспособность информационной системы быть восстановлена при обычных обстоятельствах в течение 3 часов после ошибки при профилактических работах с оборудованием?
- Может ли работоспособность информационной системы быть восстановлена при обычных обстоятельствах в течение одного часа после ошибки при профилактических работах с оборудованием?
- Может ли работоспособность информационной системы быть

восстановлена при обычных обстоятельствах в течение 15 минут после ошибки при профилактических работах с оборудованием?
- Может ли ошибка при профилактических работах с оборудованием привести к утечке информации к поставщикам услуг?
- Может ли ошибка при профилактических работах с оборудованием привести к утечке информации к сотрудникам?

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

- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение 3 часов после ошибки при профилактических работах с ПО?
- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение одного часа после ошибки при профилактических работах с ПО?
- Может ли работоспособность системы быть восстановлена при обычных обстоятельствах в течение 15 минут после ошибки при профилактических работах с ПО?
- Может ли ошибка при профилактических работах с ПО привести к утечке информации к посторонним лицам?
- Может ли ошибка при профилактических работах с ПО привести к утечке информации к поставщикам услуг?
- Может ли ошибка при профилактических работах с ПО привести к утечке информации к сотрудникам?
- Может ли ошибка при профилактических работах с ПО привести к незначительному искажению информации?
- Может ли ошибка при профилактических работах с ПО привести к обширному искажению информации?
- Можно ли обнаружить ошибки в данных?

Угроза: **Ошибки пользователей**

- Может ли работоспособность информационной системы быть

восстановлена при обычных обстоятельствах в течение 15 минут после ошибки пользователя?

- Может ли ошибка пользователя привести к утечке информации к посторонним лицам?
- Может ли ошибка пользователя привести к утечке информации к сотрудникам?
- Может ли ошибка пользователя привести к незначительному искажению информации?
- Можно ли обнаружить ошибки в данных?

Угроза: **Пожар**

- Какова конструкция здания?
- Располагаются ли снаружи на стенах здания горючие архитектурные или декоративные элементы (например, деревянная обшивка, вывески, здание оплетено виноградом и т.п.)?
- Поддерживаются ли помещения в должном техническом состоянии (например, хорошо ли подогнаны окна и двери)?
- Хранятся, используются и переносятся ли в непосредственной близости от ответственного оборудования, относящегося к информационной системе, горючие материалы – например, растворители, бумажные отходы, упаковочные материалы? (Речь не идет о небольших количествах вышеперечисленных материалов, используемых при повседневной работе.)
- С какой скоростью может распространяться огонь в здании (примите во внимание наличие открытых пространств, вентиляционных и иных шахт и отверстий в потолках и стенах)?
- Остались ли невыполненными какие-либо рекомендации или требования, высказанные при последнем визите инспектором по противопожарной безопасности?
- Через какое время после вызова может приехать пожарная команда?
- Насколько серьезно скажется на деятельности организации

пожар в месте расположения информационной системы?

Угроза: **Затопление**

- Поддерживаются ли помещения, в которых установлено ответственное оборудование информационной системы, в должном техническом состоянии (хорошо ли подогнаны окна и двери, не протекают ли трубы и т.п.)?
- Установлено ли ответственное оборудование информационной системы в помещениях, расположенных ниже уровня грунтовых вод?
- Установлено ли ответственное оборудование информационной системы в подвальных или полуподвальных помещениях?
- Насколько серьезно скажется затопление на деятельности организации?

Угроза: **Природные катаклизмы**

- Насколько серьезно скажется воздействие природных катаклизмов на деятельности организации?

Угроза: **Нехватка персонала**

- Сколько ключевых сотрудников должно отсутствовать для того, чтобы работа застопорилась?
- Насколько серьезно скажется отсутствие ключевых сотрудников в течение одного дня или менее на деятельности организации? (Из возможных вариантов выберите ответ с максимальным количеством баллов.)
- Насколько серьезно скажется отсутствие ключевых сотрудников в течение недели или менее на деятельности организации? (Из возможных вариантов выберите ответ с максимальным количеством баллов.)
- Насколько серьезно скажется отсутствие ключевых сотрудников в течение недели и более на деятельности

организации? (Из возможных вариантов выберите ответ с максимальным количеством баллов.)

- Легко ли набрать персонал, способный обслуживать ответственные компоненты системы?

Угроза: **Кражи со стороны сотрудников**

- Проводится ли расследование всех случаев краж в организации?
- Используются ли в системе устройства, которые можно легко вынести за пределы здания?
- Насколько серьезно скажется кража оборудования на деятельности организации?
- Возможна ли замена ответственного оборудования?
- Необходимо ли получить письменное разрешение на вынос оборудования из здания?
- Могут ли люди находиться на рабочих местах в нерабочее время (речь идет о сотрудниках, уборщиках, лицах, работающих по контракту)?

Угроза: **Кражи со стороны посторонних**

- Расположено ли здание на территории, где возникают сложности с поддержанием правопорядка?
- Используются ли в системе устройства, которые можно легко вынести за пределы здания?
- Насколько серьезно скажется кража оборудования на деятельности организации?
- Возможна ли замена ответственного оборудования?
- Контролируется ли доступ в здание (секретарем в приемной, охранниками и т.п.)?
- Сколько входов и выходов в здании?
- Сопровождают ли посетителей организации?
- Могут ли посетители проходить в здание (на территорию, занимаемую организацией) в нерабочее время?

Угроза: **Преднамеренное вредительство со стороны сотрудников**

- Разрешено ли сотрудникам работать в помещениях (в зоне расположения компонентов системы) в нерабочее время?
- Находятся ли в помещении (в зоне расположения компонентов системы) при обычных обстоятельствах два человека и более?
- Все ли сотрудники подвергаются тщательной проверке при приеме на работу?
- Насколько серьезно скажется поломка устройств, относящихся к информационной системе, на деятельности организации?

Угроза: **Преднамеренное вредительство со стороны посторонних**

- Могут ли обычные граждане проходить рядом со зданием или на небольшом расстоянии от него?
- Имеются ли на первом этаже здания большие застекленные окна?
- Присутствуют ли люди в здании круглосуточно?
- Разрешен ли обычным гражданам свободный доступ в здание?
- Насколько серьезно скажется поломка устройств, относящихся к информационной системе, на работе пользователей?
- Уязвимы ли для нападения жизненно важные внешние системы, обслуживающие здание (линии энергоснабжения, например)?

Угроза: **Терроризм**

- Могут ли обычные граждане проходить рядом со зданием или на небольшом расстоянии от него?
- Могут ли обычные граждане парковать свои машины со зданием или на небольшом расстоянии от него?
- Используется ли здание совместно с другими

организациями?

- Разрешен ли обычным гражданам доступ в здание?
- Доставляются ли в здание вне какого-либо расписания посылки, контейнеры и т.п. неизвестного происхождения?
- Насколько серьезно нападение на здание террористов или экстремистов на деятельности организации?
- Существует ли у кого-либо из сотрудников конфликт интересов с экстремистской или террористической организацией и не связан ли кто-нибудь из них с подобной организацией?
- Расположено ли здание организации в стране, где существуют проблемы с поддержанием законности и порядка?