ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

Государственное бюджетное профессиональное образовательное учреждение г. Москвы Колледж связи № 54 им. П.М.Вострухина

ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

"БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ"

РАЗДЕЛ 2. Обеспечение безопасности информационных технологий" Тема 3. Планы защиты и планы обеспечения непрерывной работы и восстановления процессов автоматизированной системы

МОСКВА 2016

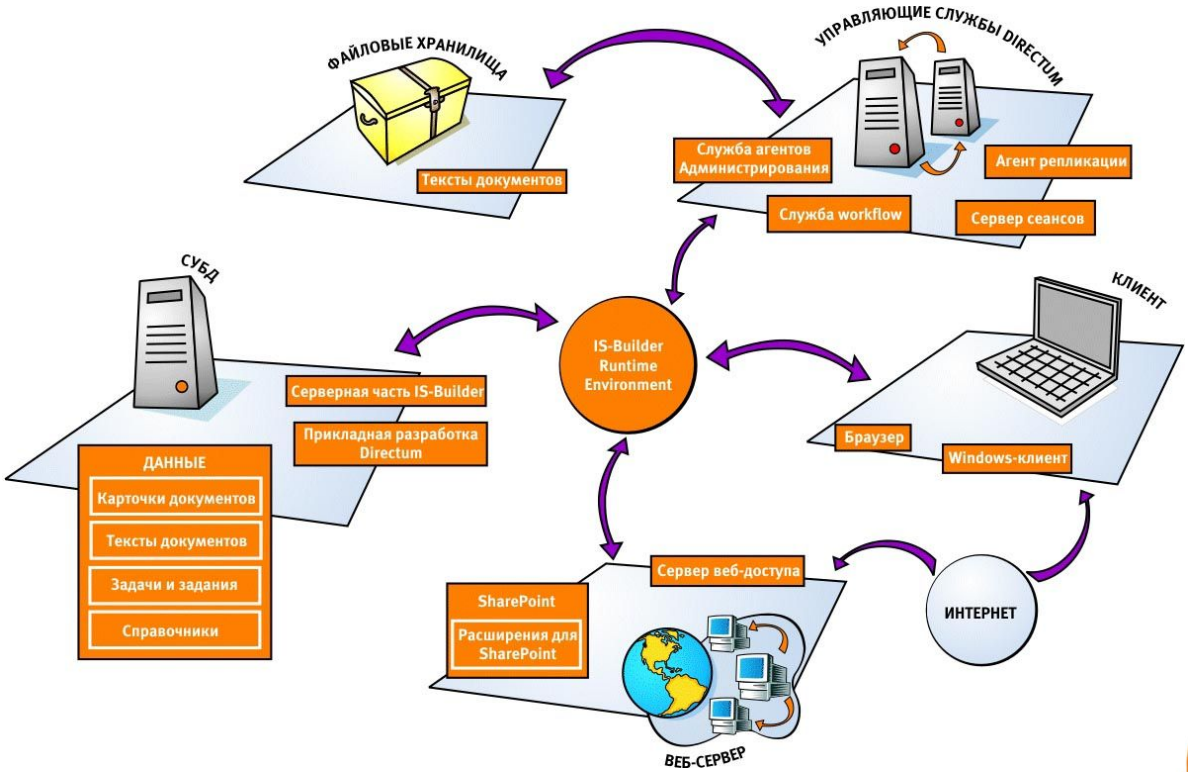
ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

План защиты информации

План защиты информации разрабатывается с целью конкретизации положений Концепции безопасности информационных технологий для конкретных подсистем АС.

Содержит:

1. Описание подсистемы АС

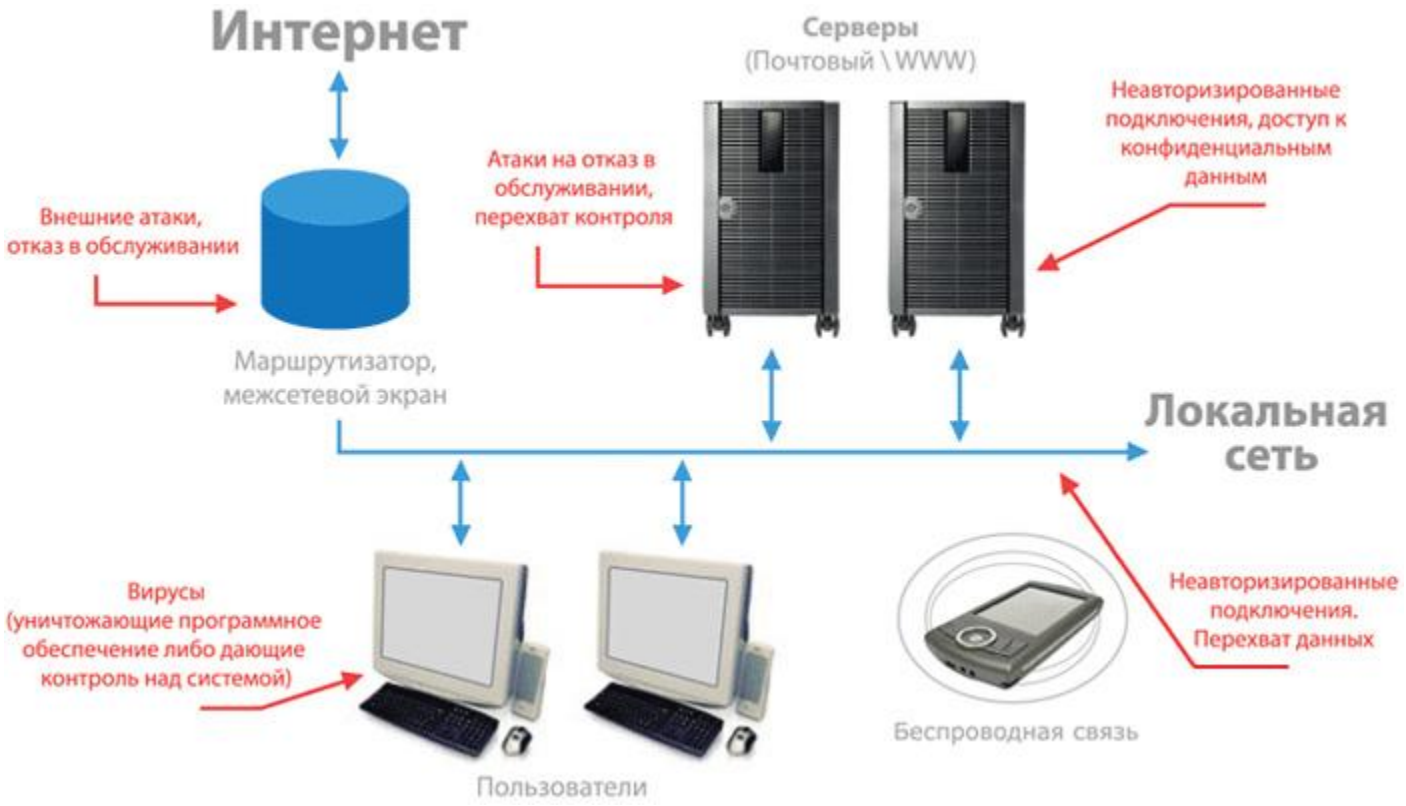


Лаборатория Информационной Безопасности

План защиты информации

2. Цель защиты и пути обеспечения безопасности ресурсов подсистемы АС и циркулирующей в ней информации

3. Перечень значимых угроз безопасности и наиболее вероятных путей нанесения ущерба подсистеме АС

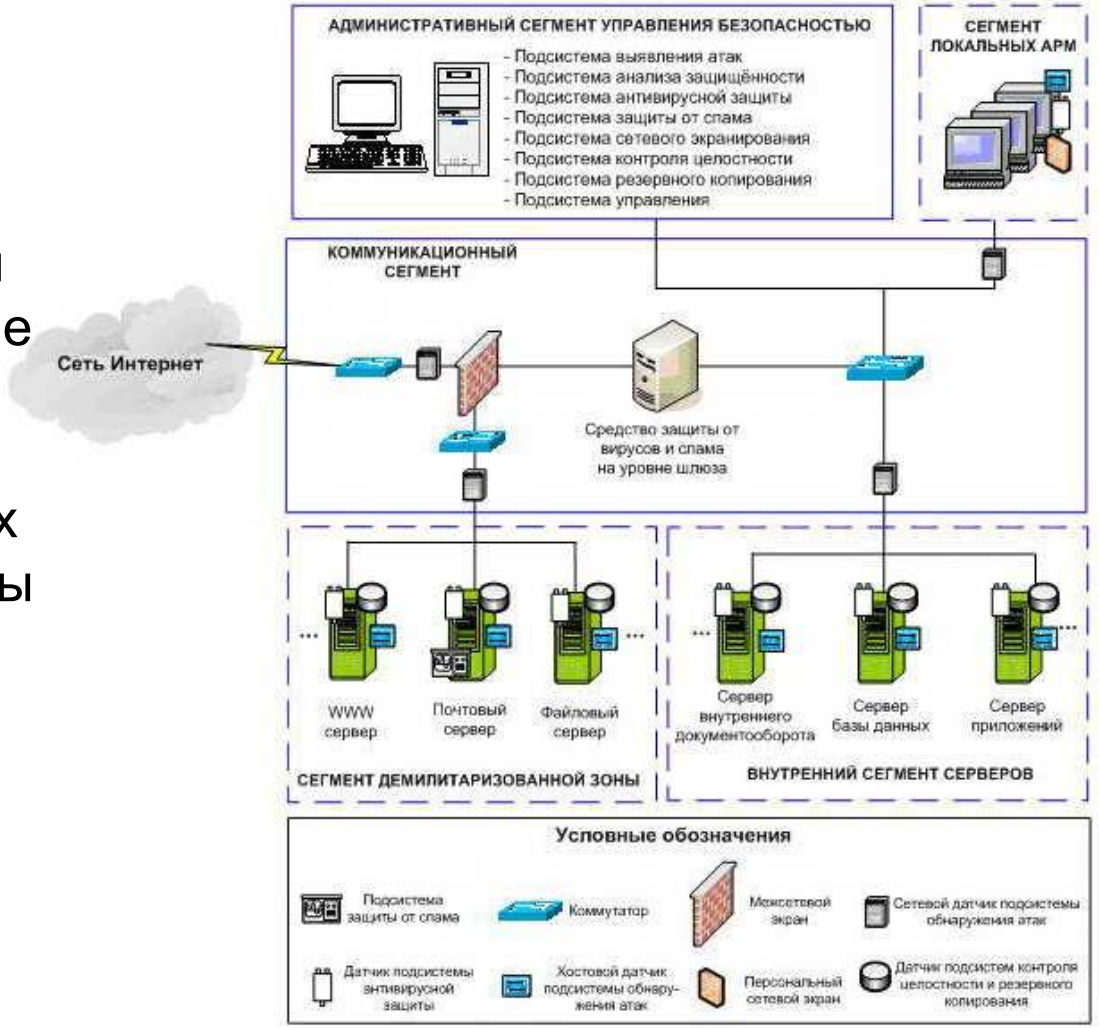


4. Основные требования к организации процесса функционирования подсистемы АС и мерам обеспечения безопасности обрабатываемой информации

5. Основные правила, регламентирующие деятельность пользователей и персонала по вопросам обеспечения безопасности в подсистеме

План защиты информации

6. Требования к условиям применения и определение зон ответственности установленных в системе штатных и дополнительных технических средств защиты



План обеспечения непрерывной работы и восстановления

План обеспечения непрерывной работы и восстановления (ПОНРВ) **определяет** основные меры, методы и средства сохранения (поддержания) работоспособности АС при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности АС и ее основных компонентов.

Кроме того, он **описывает** действия различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба

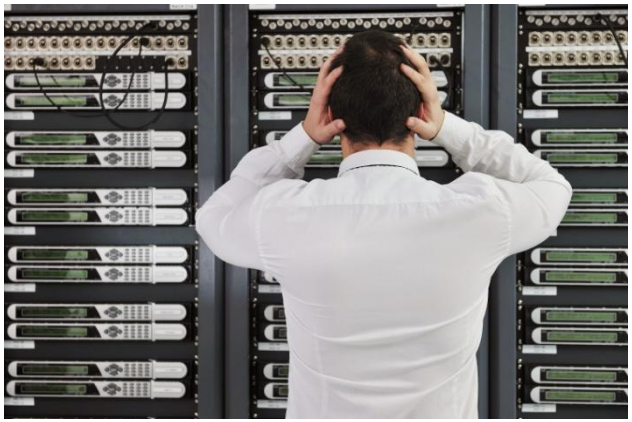
Классификация кризисных ситуаций по степени серьезности

Кризисная ситуация

Угрожающая	Серьезная	Требующая внимания
Приводящая к полному выходу АС из строя и ее неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправо-мерной модификации или компрометации наиболее важной информации	Приводящая к выходу из строя отдельных компонентов системы, потере производитель-ности, а также к нарушению целост-ности и конфиденци-альности программ и данных в результате НСД	Не приводящие к ощутимому ущербу, но требующие адекватной реак-ции (неудачные попытки НСД)

Угрожающие кризисные ситуации

1. Нарушение подачи электроэнергии в здание



2. Выход из строя сервера
(с потерей информации)

3. Выход из строя сервера
(без потери информации)

Угрожающие кризисные ситуации

4. Частичная потеря информации на сервере без потери его работоспособности

5. Выход из строя локальной сети (физической среды передачи данных)

Серьезные кризисные ситуации

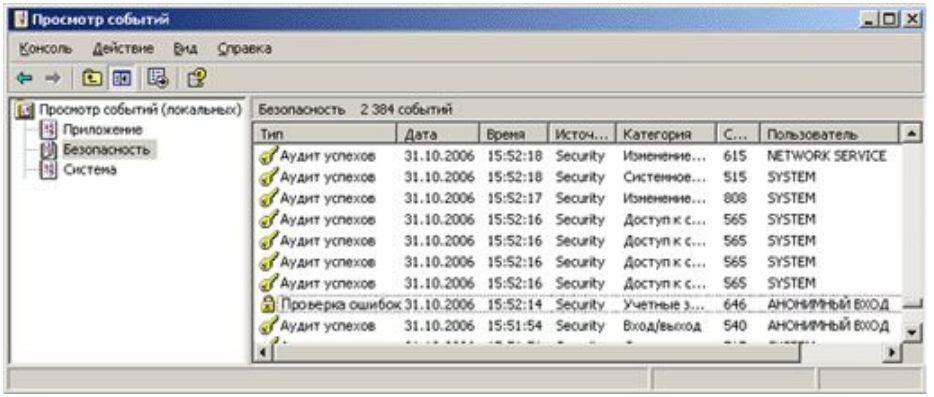
1. Выход из строя рабочей станции (с потерей информации)

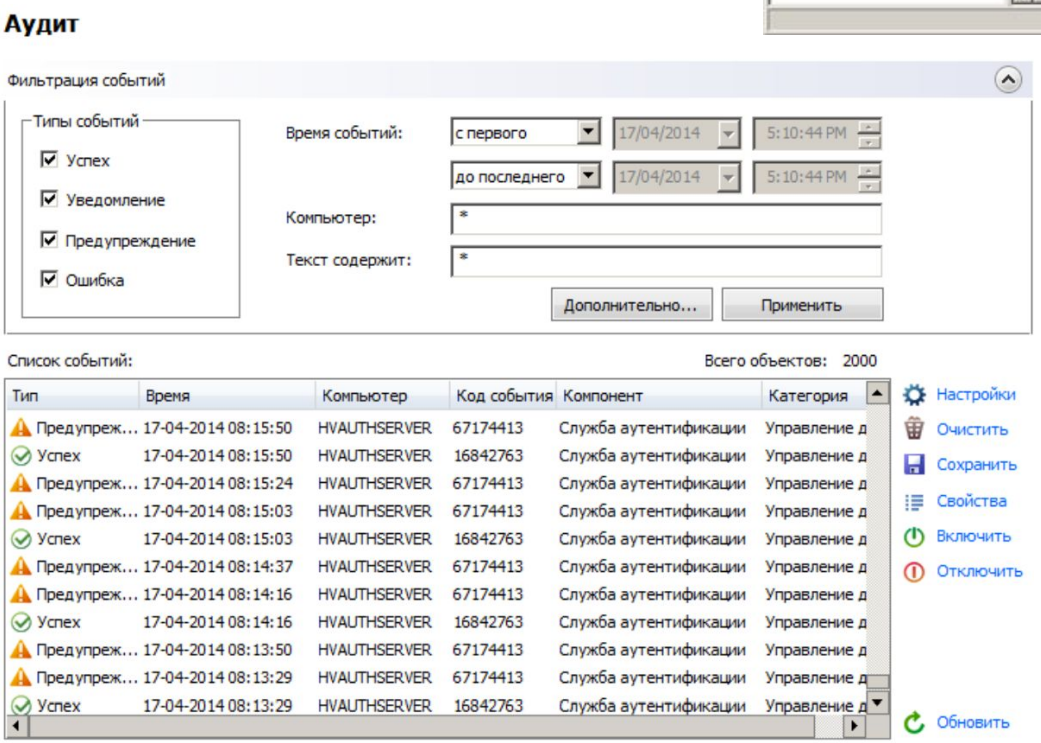
2. Выход из строя рабочей станции (без потери информации)

3. Частичная потеря информации на рабочей станции без потери ее работоспособности

Ситуации, требующие внимания

Несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации





Лаборатория Информационной Безопасности

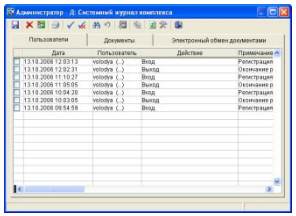
Источники информации

Пользователи, обнаружившие несоответствия Плану защиты или другие подозрительные изменения

Средства защиты, обнаружившие предусмотренную планом защиты кризисную ситуацию

Источники информации о возникновении кризисной ситуации

Системные журналы, в которых имеются записи, свидетельствующие о возникновении кризисной ситуации



Меры ОНРВ автоматизированных систем

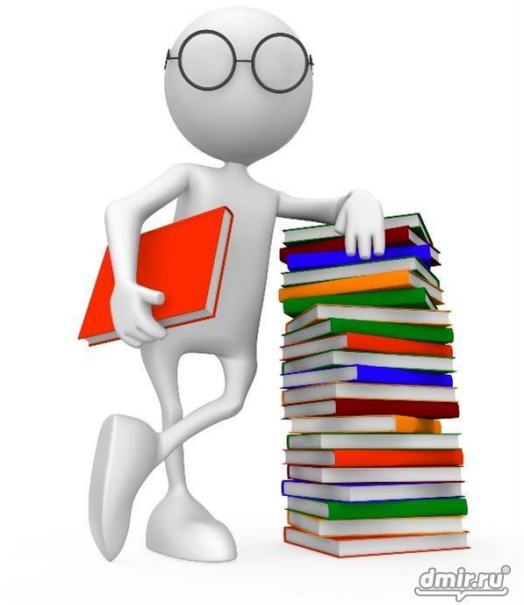
Непрерывность процесса **функционирования** АС и **своевременность восстановления** ее работоспособности достигается:

1. Проведение специальных организационных мероприятий и разработка организационно-распорядительных документов

2. Регламентация процесса обработки информации с применением ЭВМ и действий персонала

Меры ОНРВ автоматизированных систем

3. Назначение и подготовка должностных лиц, отвечающих за организацию и осуществление практических мероприятий



4. Четкое знание и строгое соблюдение требований руководящих документов по обеспечению НРВ

Меры ОНРВ автоматизированных систем

5. Применение различных способов резервирования, эталонного и страхового копирования ресурсов системы

6. Контроль за соблюдением требований по обеспечению НРВ

Лаборатория Информационной Безопасности

Меры ОНРВ автоматизированных систем

7. Постоянное поддержание необходимого уровня защищенности компонентов системы, непрерывное управление применением средств защиты

8. Проведение постоянного анализа эффективности принятых мер и применяемых способов и средств обеспечения НРВ

Обязанности и действия персонала по обеспечению НРВ автоматизированной системы

Действия персонала в кризисной ситуации зависят от степени ее тяжести.

В случае возникновения **ситуации требующей внимания**, администратор безопасности подсистемы должен провести ее анализ собственными силами.

О факте систематического возникновения таких ситуаций и принятых мерах необходимо ставить в известность руководство подразделения.

Обязанности и действия персонала по обеспечению НРВ автоматизированной системы

В случае возникновения **угрожающей** или **серьезной** критической ситуации, действия персонала включают следующие **этапы**:

- немедленная реакция;

- частичное восстановление работоспособности и возобновление обработки;

- полное восстановление системы и возобновление обработки в полном объеме;

- расследование причин кризисной ситуации и установление виновных.

Лаборатория Информационной Безопасности

1. Немедленная реакция.

Ответственные за этап: оператор подсистемы и администратор безопасности.

Действия:

- оператор обязан немедленно оповестить администратора безопасности о факте возникновения кризисной ситуации;
- администратор должен поставить в известность операторов всех смежных подсистем для их перехода на аварийный режим работы (приостановку работы);
- вызвать ответственных системного программиста и системного инженера;
- определить степень серьезности и масштабы кризисной ситуации, размеры и область поражения;
- оповестить персонал взаимодействующих подсистем о характере кризисной ситуации и ориентировочном времени возобновления обработки.

2. Частичное восстановление работоспособности.

Ответственные за этап: администратор безопасности подсистемы, системный программист и системный инженер.

Действия:

- отключить пораженные компоненты или переключиться на использование дублирующих ресурсов;
- если не произошло повреждения программ и данных, возобновить обработку и оповестить об этом персонал взаимодействующих подсистем;
- восстановить работоспособность поврежденных критичных аппаратных средств и другого оборудования;
- восстановить поврежденное критичное программное обеспечение;
- проверить работоспособность поврежденной подсистемы;
- уведомить операторов смежных подсистем о готовности к работе.

3. Полное восстановление в период неактивности системы.

Ответственные за этап: администратор безопасности подсистемы, системный программист и системный инженер.

Действия:

- восстановить работоспособность всех поврежденных аппаратных средств;
- восстановить и настроить все поврежденные программы;
- восстановить все поврежденные данные;
- настроить средства защиты подсистемы в соответствии с планом защиты;
- о результатах восстановления уведомить администратора системы (базы данных)

4. Расследование причин возникновения кризисной ситуации.

Ответственные за этап: администратор безопасности подсистемы.

Действия:

Получить ответы на вопросы:

- случайная или преднамеренная кризисная ситуация?
- учитывалась ли возможность ее возникновения в Плане защиты и Плане ОНРВ?
- можно ли было ее предусмотреть?
- вызвана ли она слабостью средств защиты и регистрации?
- превысил ли ущерб от нее установленный уровень?
- есть ли невосполнимый ущерб и велик ли он?
- это первая кризисная ситуация такого рода?
- есть ли возможность точно определить круг подозреваемых?
- есть ли возможность точно установить виновника?
- в чем причина кризисной ситуации?
- достаточно ли имеющегося резерва?
- есть ли необходимость пересмотра Плана защиты?
- есть ли необходимость пересмотра Плана ОНРВ?

Обязанности системного инженера по обеспечению НРВ автоматизированной системы

Системный инженер обязан:

- поддерживать аппаратные средства и другое оборудование, включая резервное, в рабочем состоянии и осуществлять периодическую их проверку;

- восстанавливать функции аппаратных средств и другого оборудования в случае отказов;

- оперативно заменять дефектные узлы резервными в случае отказов;

- подготавливать и оперативно включать резервные аппаратные средства и другое оборудование в случае серьезной кризисной ситуации.

Контрольные вопросы

Контрольные вопросы:

1. Содержание Плана защиты информации.
2. Что определяет и что описывает План обеспечения непрерывной работы и восстановления?
3. Классификация кризисных ситуаций по степени серьезности.
4. Перечислите угрожающие кризисные ситуации в результате нежелательного воздействия на АС.
5. Перечислите серьезные кризисные ситуации в результате нежелательного воздействия на АС.
6. Назовите источники информации о возникновении кризисной ситуации в результате нежелательного воздействия на АС.
7. Чем достигается непрерывность процесса функционирования АС и своевременность восстановления ее работоспособности?

Лаборатория Информационной Безопасности

Контрольные вопросы

Контрольные вопросы:

8. Назовите этапы действий персонала в случае возникновения угрожающей или серьезной критической ситуации в результате нежелательного воздействия на АС.

9. Действия персонала в качестве немедленной реакции при возникновении угрожающей или серьезной критической ситуации в результате нежелательного воздействия на АС.

10. Действия персонала для частичного восстановления работоспособности при возникновении угрожающей или серьезной критической ситуации в результате нежелательного воздействия на АС.

11. Действия персонала для полного восстановления работоспособности при возникновении угрожающей или серьезной критической ситуации в результате нежелательного воздействия на АС.

12. Обязанности системного инженера по обеспечению НРВ автоматизированной системы.

Лаборатория Информационной Безопасности

Спасибо за внимание!

Лаборатория Информационной Безопасности