Организационные методы защиты информации. Создание и поддержание инфраструктуры защиты информации в организации

ЛЮБЧИК ДМИТРИЙ СЕРГЕЕВИЧ

Методы защиты информации

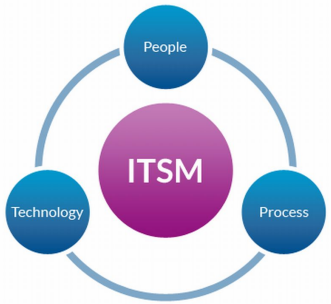
Международные стандарты

COBIT 5

ISO 27000

NIST
National Institute of Standards and Technology
Center of Excellence

ITIL®



Международные стандарты

Серия СТБ ISO/IEC 27000


План
Внедрение
Внедрение
Проверка
(Аудит)
Улучшение
Внедрение СУИБ

Законодательство РБ в области защиты информации

Документация на систему защиты информации

Политика в отношении мобильных устройств

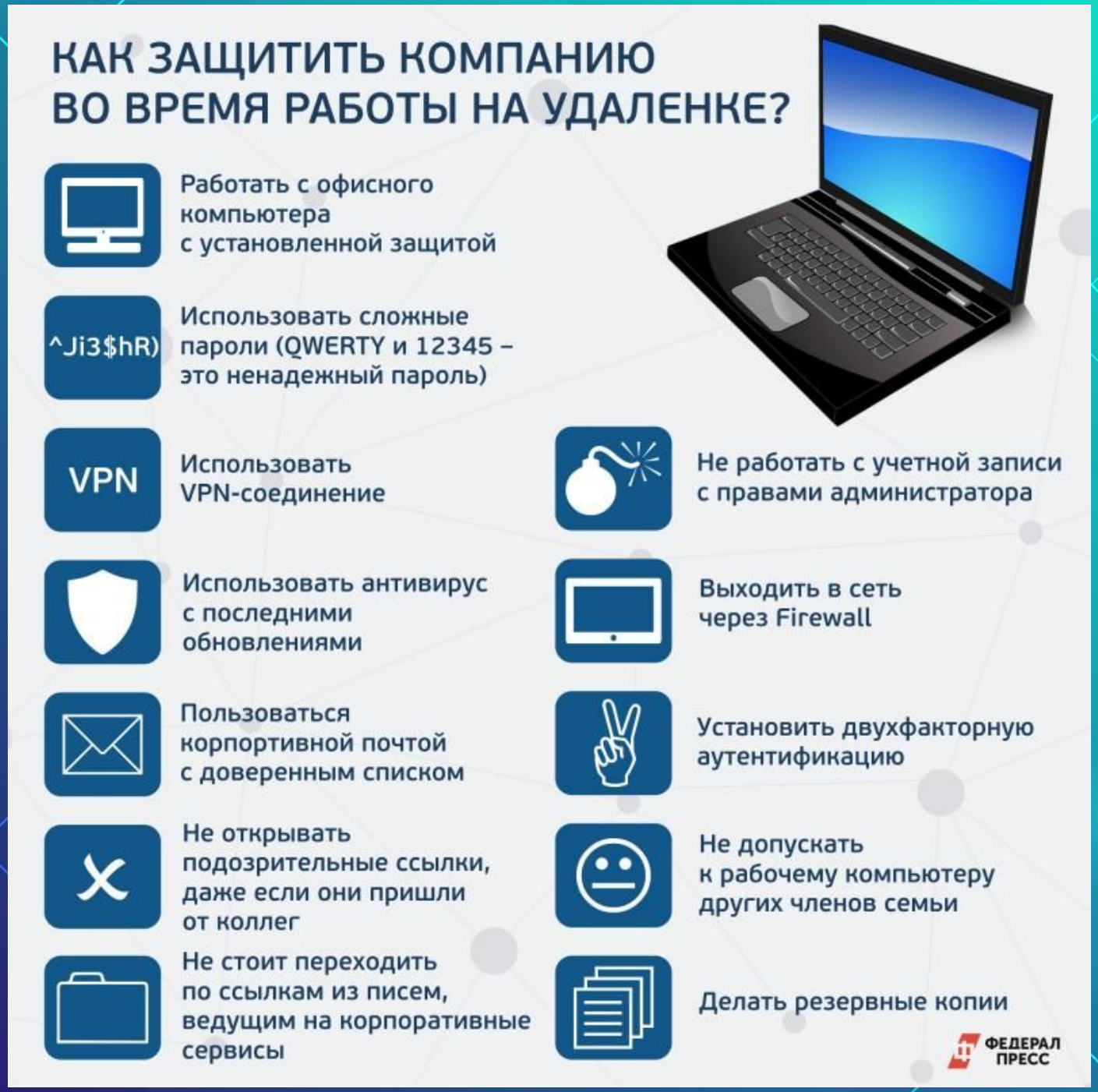
Метод реализации

- Должны быть приняты политика и меры по обеспечению безопасности для управления рисками, связанными с использованием мобильных устройств.

Удаленная работа

Метод реализации

- Должны быть приняты политика и меры обеспечения безопасности для защиты информации, к которой осуществляется доступ на удаленных рабочих местах и которая там обрабатывается или сохраняется.



Управление съемными носителями информации

Метод реализации

- Должны быть внедрены процедуры для управления съемными носителями в соответствии со схемой классификации, принятой в организации

Bad USB

класс хакерских атак, основанный на уязвимости USB устройств. Благодаря отсутствию защиты от перепрошивки в некоторых USB-устройствах, злоумышленник может видоизменить или полностью заменить оригинальную прошивку и заставить устройство имитировать любое другое устройство. BadUSB предназначен для доставки и исполнения вредоносного кода

Киберпреступная группировка FIN7

Киберпреступная группировка FIN7 последние несколько месяцев отправляла вредоносные USB-устройства американским компаниям с целью заразить их компьютерные системы вымогательским ПО.

С августа 2021 года ФБР получило сообщения о нескольких посылках, содержащих эти USB-устройства, которые были отправлены американским предприятиям в сфере транспорта, страхования и обороны.

Политика контроля доступа

Рекомендации по применению

- Владельцы активов должны определить соответствующие правила для контроля доступа, права доступа и ограничения для определенных категорий пользователей по отношению к их активам с уровнем детализации и строгости контроля, отражающей риски, связанные с информационной безопасностью
- Категорически запрещен доступ к ресурсам по принципу «Всем – Полный доступ».

Защита от вредоносного ПО

Назначение

- Предназначен для определения правил и способов защиты информационных средств от вредоносного ПО
- Защита от вредоносного кода должна основываться на применении программ обнаружения вредоносного кода и восстановления, осведомленности об информационной безопасности и соответствующих средствах контроля доступа к системе и управлению изменениями

Резервное копирование информации

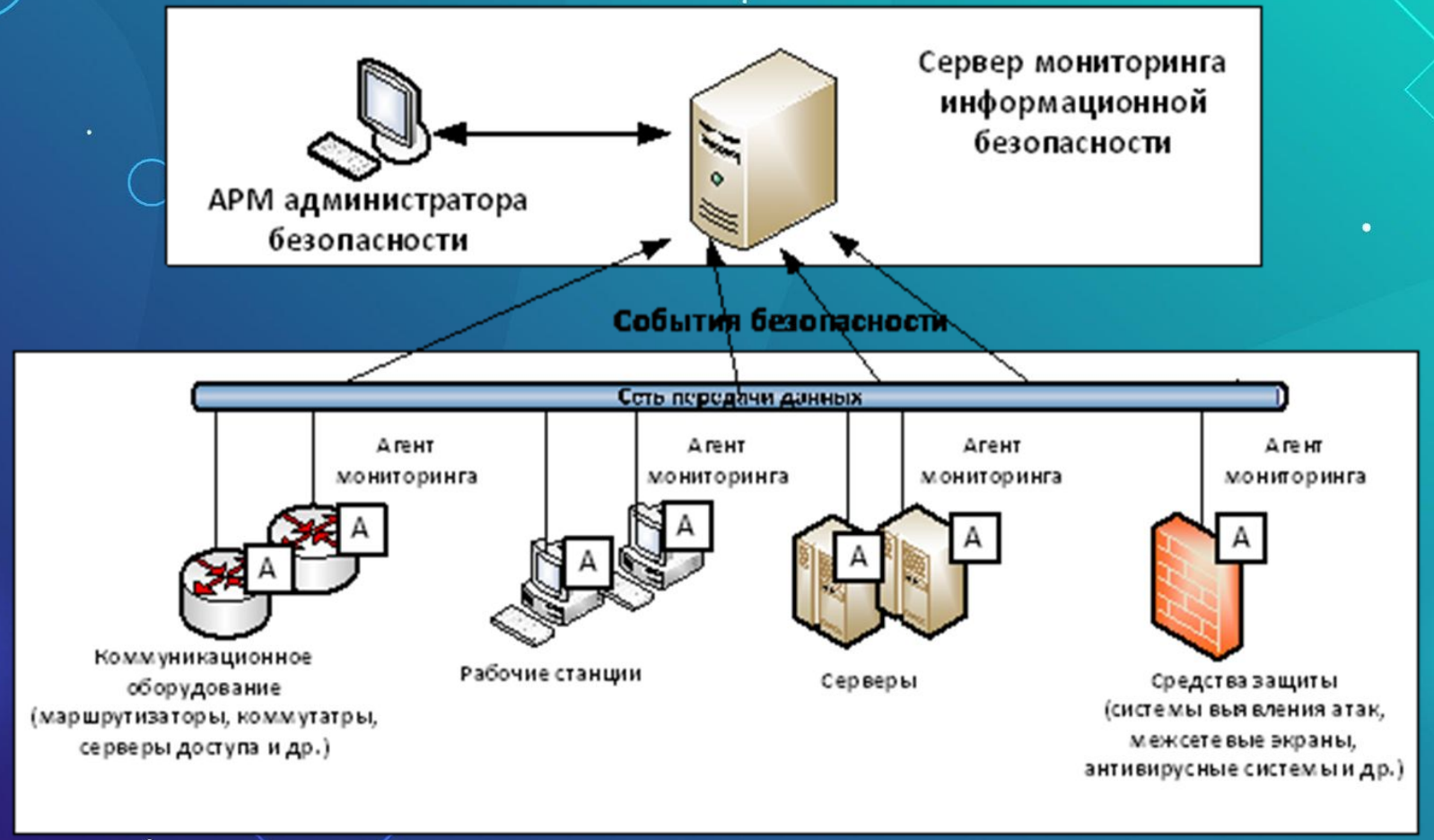
Задача

- обеспечить защиту от потери данных

Мониторинг за функционированием информационной системы

Назначение

- Предназначен для определения правил по мониторингу за функционированием информационной системы



Использование электронной почты

Назначение

- Предназначен для определения правил работы с электронной почтой

Использование электронной почты

Как узнать фишинговое письмо

1. **Вы не ждали это письмо**

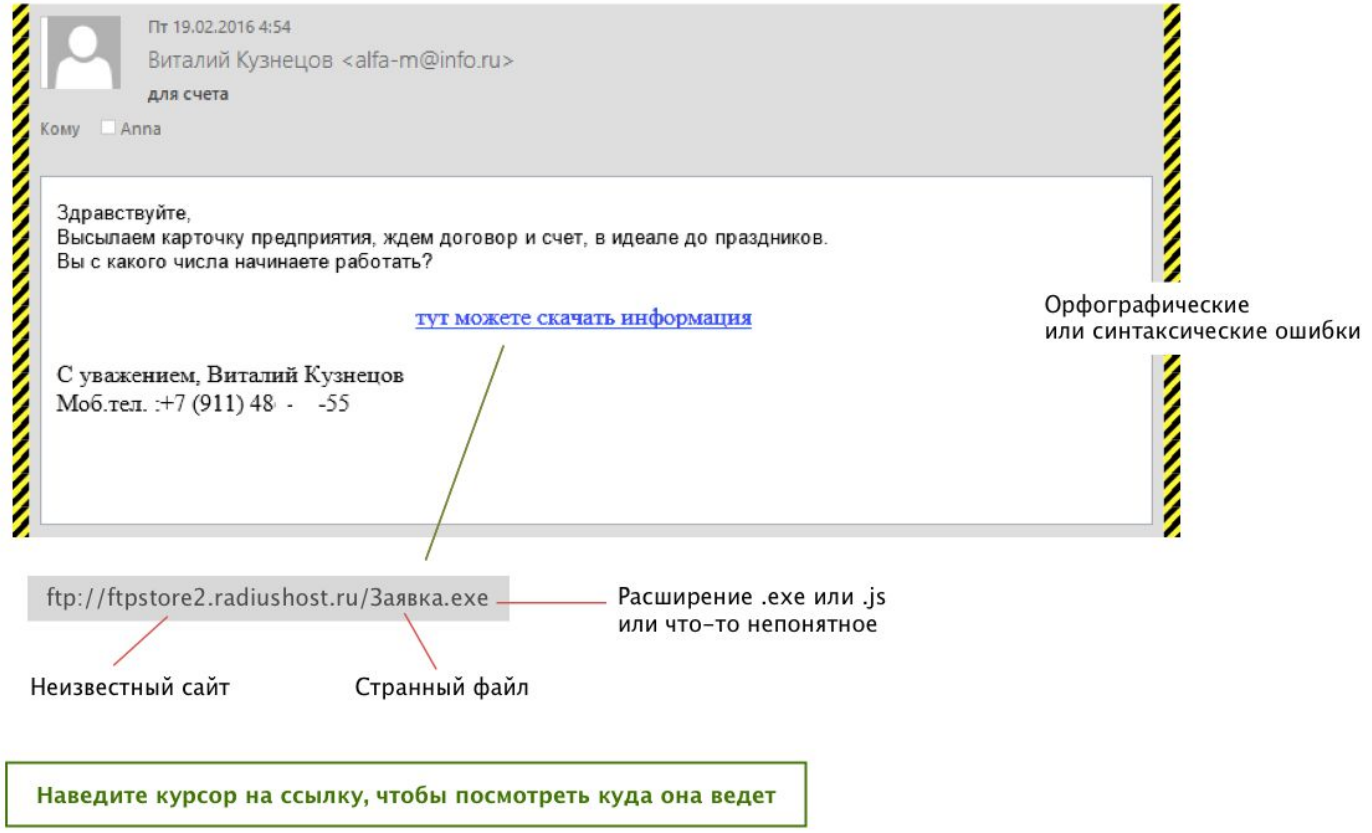
   Вы не знаете отправителя лично

2. **В письме — проблема или срочный вопрос**

   Вы узнали о проблеме из этого письма

   От вас требуется срочное действие

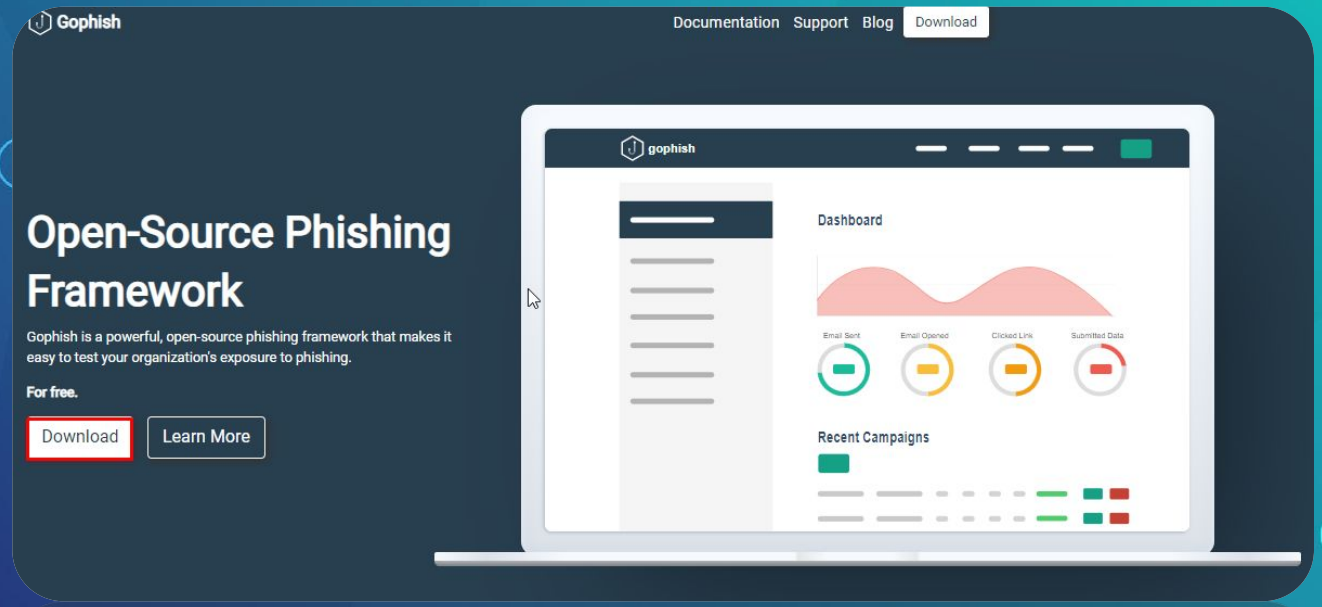
3. **Вас просят перейти по ссылке**



Наведите курсор на ссылку, чтобы посмотреть куда она ведет

Обучение сотрудников (Gophish)

Gophish — фреймворк, который позволяет проверить реакцию сотрудников компании на фишерские послания.



В Гродно одно из предприятий потеряло более 70 тысяч рублей из-за электронного письма

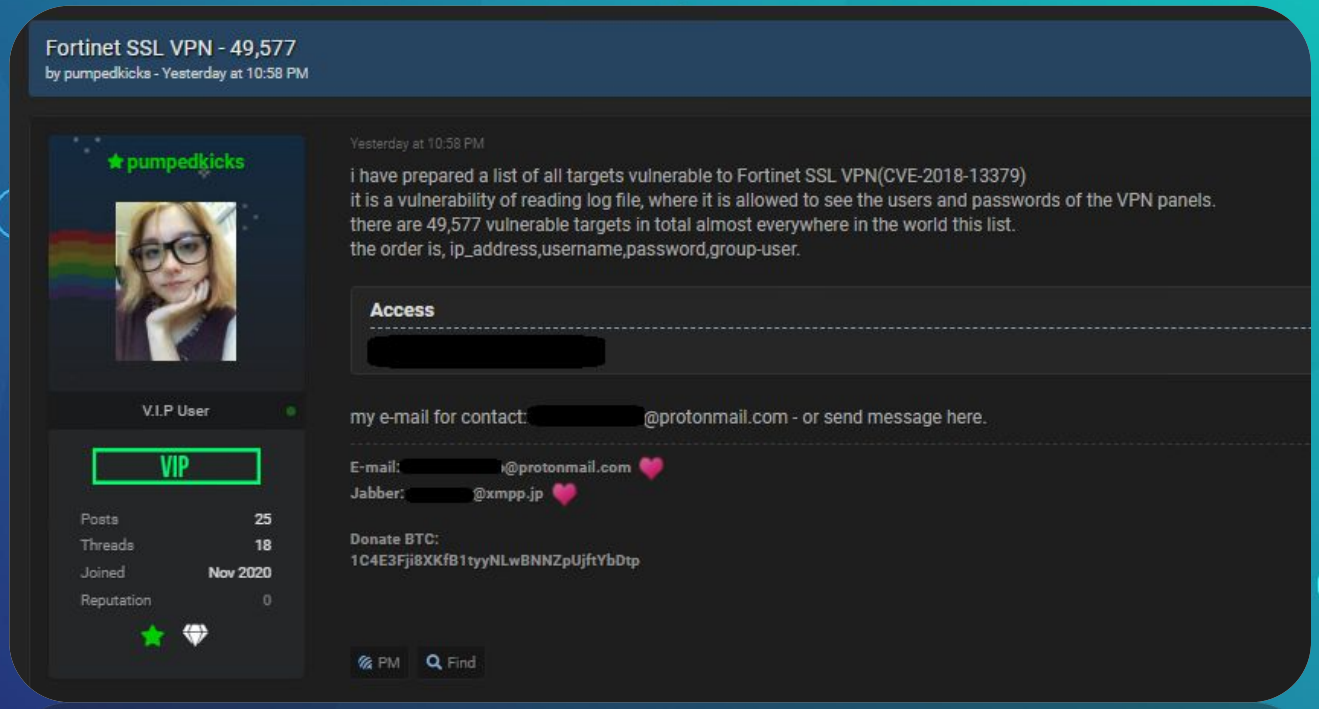
«Внешне адрес электронной почты был максимально схож с адресом поставщика. Сотрудники предприятия не обратили внимания на минимальные отличия, полагая, что реквизиты действительно поменялись, и добросовестно отправили туда внушительную сумму — более 70 тыс. рублей», — рассказали в милиции.

Обновление программного обеспечения

Fortinet VPN

На подпольном форуме RAMP бесплатно доступен массив, содержащий почти 500 тыс. учетных данных для устройств Fortinet VPN

Как полагают специалисты, для сбора учетных данных злоумышленники эксплуатировали уязвимость обхода каталога (CVE-2018-13379) в FortiOS SSL VPN. (новость от 9 Сентября, 2021)



Реагирование на инциденты ИБ

Задача

- гарантировать последовательный и результативный подход к управлению инцидентами информационной безопасности, включая информирование о событиях, связанных с безопасностью, и уязвимостях

ВЫВОДЫ

Создание и поддержание инфраструктуры защиты информации в организации

ПОЛОЖЕНИЕ

о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено

Комплекс мероприятий по технической и криптографической защите информации

1. Проектирование системы защиты информации
2. **Создание** системы защиты информации
3. **Аттестация** системы защиты информации
4. Обеспечение функционирования СЗИ в процессе **эксплуатации** ИС
5. Обеспечение защиты информации в случае **прекращения** эксплуатации ИС

Работы по технической и криптографической защите информации

Классы типовых информационных систем

На этапе проектирования системы защиты информации

- анализ структуры информационной системы и информационных потоков
- разработка (корректировка) политики информационной безопасности
- определение требований защиты информации в техническом задании на создание СЗИ
- выбор средств технической и криптографической защиты информации
- разработка (корректировка) общей схемы системы защиты информации

Техническое задание

Техническое задание

Общая схема системы защиты информации

СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В ходе внедрения средств технической и криптографической защиты информации

Документация на систему защиты информации

Обеспечение функционирования системы защиты информации в процессе эксплуатации

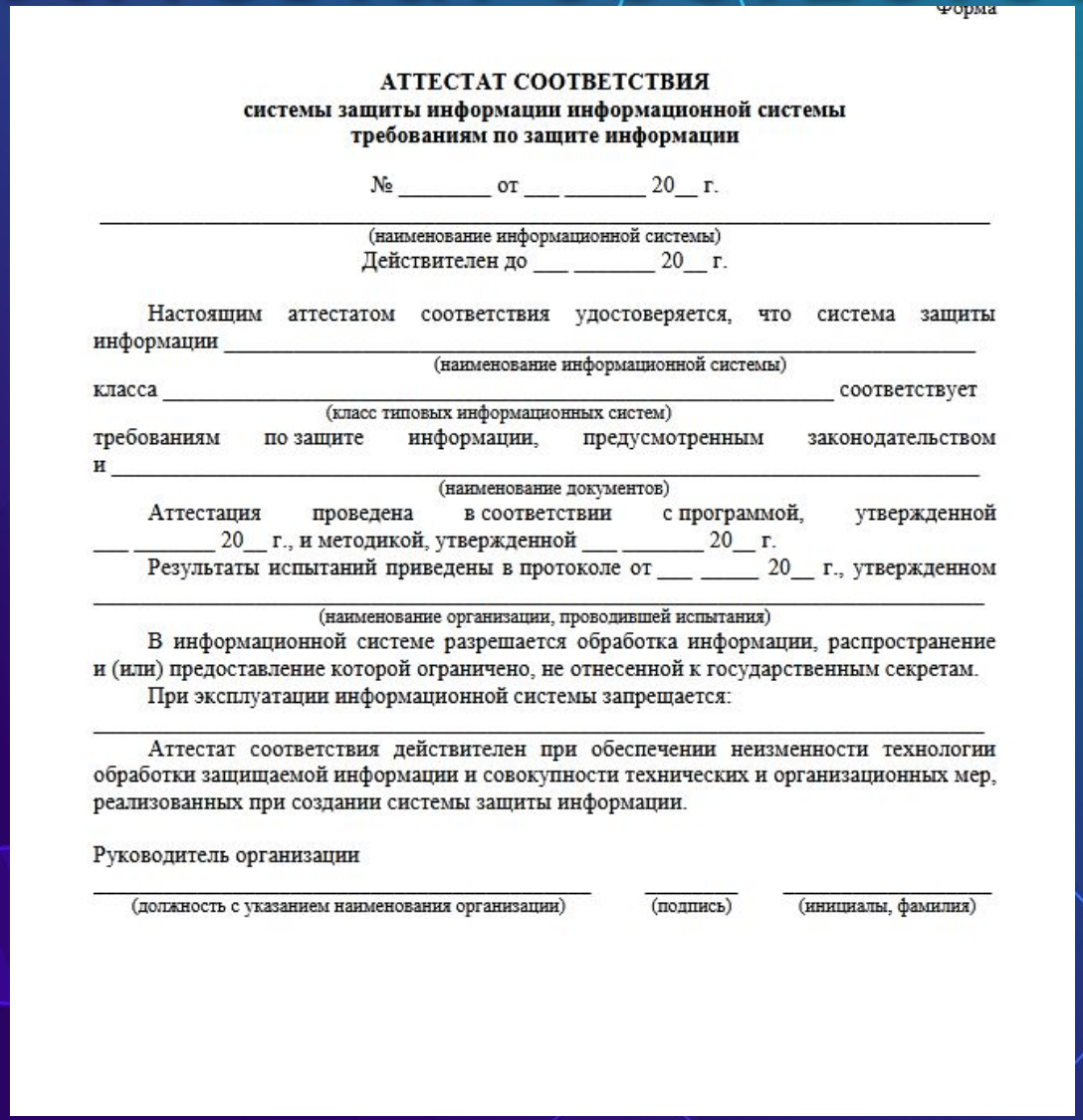
АТТЕСТАЦИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аттестация проводится в случаях

Аттестация включает:

Срок проведения аттестации

Аттестат соответствия



Форма

АТТЕСТАТ СООТВЕТСТВИЯ
системы защиты информации информационной системы
требованиям по защите информации

№ _____ от ___ _____ 20__ г.

_____
(наименование информационной системы)

Действителен до ___ _____ 20__ г.

Настоящим аттестатом соответствия удостоверяется, что система защиты информации _____
(наименование информационной системы)
класса _____ соответствует
(класс типовых информационных систем)
требованиям по защите информации, предусмотренным законодательством и _____
(наименование документов)

Аттестация проведена в соответствии с программой, утвержденной ___ _____ 20__ г., и методикой, утвержденной ___ _____ 20__ г.

Результаты испытаний приведены в протоколе от ___ _____ 20__ г., утвержденном _____
(наименование организации, проводившей испытания)

В информационной системе разрешается обработка информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

При эксплуатации информационной системы запрещается:

_____

Аттестат соответствия действителен при обеспечении неизменности технологии обработки защищаемой информации и совокупности технических и организационных мер, реализованных при создании системы защиты информации.

Руководитель организации

_____ _____ _____
(должность с указанием наименования организации) (подпись) (инициалы, фамилия)

Выдается на 5 лет

Представление в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации

Срок предоставления копий

Спасибо за внимание!