ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ФИЛИМОНОВА МАРИЯ АНДРЕЕВНА

УО БЕЛОРУССКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ СВЯЗИ

ТРИАДА CIA

- Confidentiality

Конфиденциальность — свойство ин… …упной или закрытой для неавторизованных лиц, сущностей…

- Integrity

Целостность — свойство сохранен… …активов;

- Availability

Доступность — свойство информации быть доступной и готовой к использованию по запросу авторизованного субъекта, имеющего на это право.

Информационная безопасность (information security):

Сохранение конфиденциальности, целостности и доступности информации.

К персональным данным относятся:

- Общие персональные данные
- Биометрические персональные данные
- Общедоступные персонифицированные данные
- Обезличенными персональные данные
- Специальные персональные данные

УГРОЗЫ ИБ


Уничтожение информационных объектов
Утечка информации
Искажение информации
Блокирование объекта информации

ИСТОЧНИКИ УГРОЗЫ КОНФЕДЕНЦИАЛЬНЫХ ДАННЫХ

УГРОЗЫ НАРУШЕНИЯ КОНФЕДЕНЦИАЛЬНОСТИ

- Хищение носителей информации
- Несанкционированный до ным системам
- Выполнение пользователем несанкционированных действий
- Перехват данных, передав и
- Раскрытие содержания информации

УГРОЗА НАРУШЕНИЯ ЦЕЛОСНОСТИ

- Уничтожение носителей информации
- Внесение несанкционированных изменений в программы и данные
- Установка и использование нештатного программного обеспечения
- Заражение вирусами
- Внедрение дезинформации

СРЕДСТВА ЗАЩИТЫ ИФОРМАЦИИ

Нормативные (неформальные):

- Нормативные(законодательны
- Административные(орган
- Морально-этические сред

Технические (формальные):

- Физические;
- Аппаратные;
- Программные;
- Криптографические.

АДМИНИСТРАТИВНЫЕ

- Организационные и административные меры
- Сертификация деятельности
- Аттестация субъектов или объектов
- Лицензирование
- Доступ:
  - Интернет;
  - К внешним ресурсам;
  - К электронной почте.

МОРАЛЬНО-ЭТИЧЕСКИЕ СРЕДСТВА

- Правила поведения в обществе и
- Личное отношение человека

ТЕХНИЧЕСКИЕ СЗ

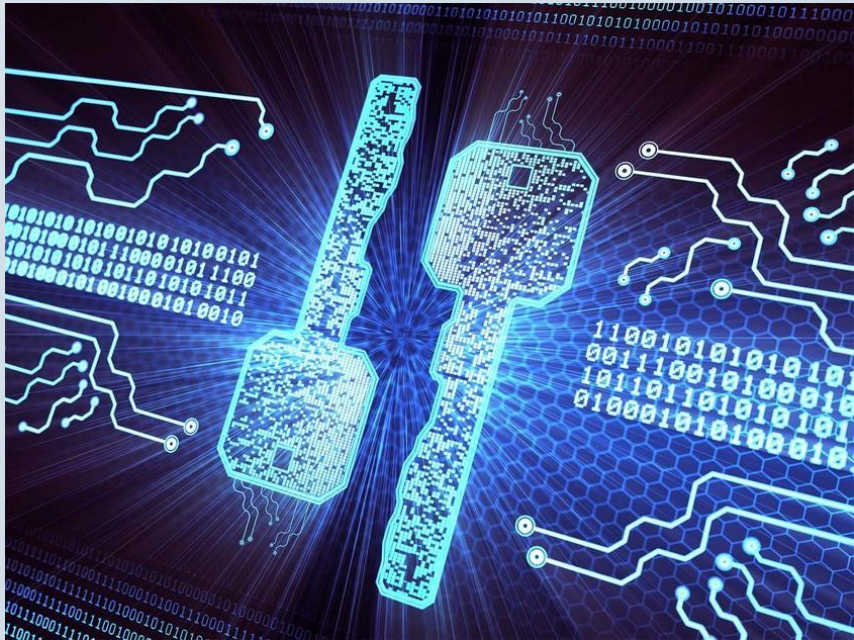
- Физические - это любые устройства, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним.
- Аппаратные - это любые устройства, которые встраиваются в информационные и телекоммуникационные системы. Они препятствуют доступу к информации, в том числе с помощью её маскировки.

Программные – это программы, предназначенные для решения задач, связанных с обеспечением информационной безопасности.

- DLP-системы - (Data Leak Prevention) служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков.

- SIEM-системы - (Security Informa ent) обеспечивают анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений.

- Криптографические – внедрение криптографических и стеганографических методов защиты данных для безопасной передачи по корпоративной или глобальной сети.



ИСТОЧНИКИ, КОТОРЫЕ УГРОЖАЮТ ИБ

- Угрозы от персонала
- Угроза от злоумышленников
- Случайное удаление данных
- Компьютерные вирусы
- Вредоносные ПО или Программные закладки
- Отказ в работе операционной истемы
- Природный фактор (пожары, наводнения, аварии в энергосистемах и т.д.)

УГРОЗЫ ОТ ПЕРСОНАЛА

ВНУТРЕННИЕ НАРУШИТЕЛИ

УГРОЗЫ ОТ ЗЛОУМЫШЛЕННИКОВ

- Злоумышленник (attacker): Любое лицо, намеренно использующее уязвимости технических и нетехнических средств безопасности в целях захвата или компрометации информационных систем и сетей или затруднения доступа авторизованных пользователей к ресурсам информационной системы и сетевым ресурсам.
- Злоумышленник: Лицо, заинтересованное в получении возможности несанкционированного доступа к конфиденциальной информации, представляющей промышленную и коммерческую тайну, предпринимающее попытку такого доступа или совершившее его.

ХАКЕР

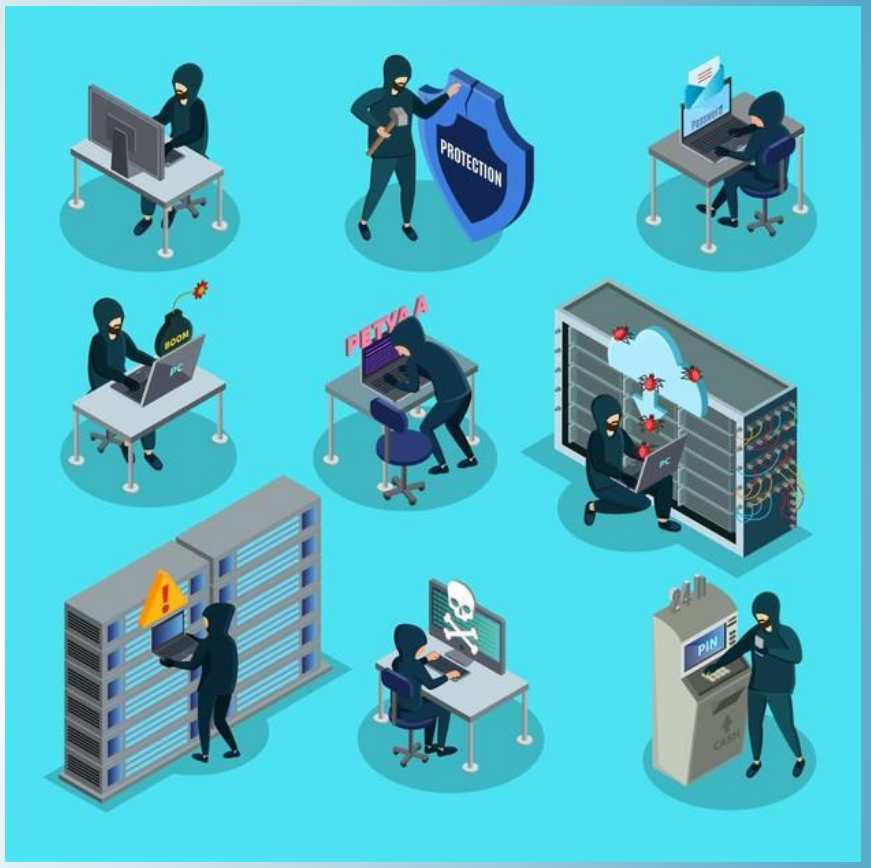
- Хакер – HACKER сущ.
- Индивидуум, который получает удовольствие от изучения деталей функционирования компьютерных систем и от расширения их возможностей, в отличие от большинства пользователей компьютеров, которые предпочитают знать только необходимый минимум.
- Энтузиаст программирования; индивидуум, получающий удовольствие от самого процесса программирования, а не от теоретизирования по этому поводу.

КРЭКЕР – CRACKERS

1. Взламывает чужие вычислительные системы и крадет чужую информацию.

МОТИВАЦИЯ

- Вымогательство
- Охота за данными
- Перехват пользовательского трафика
- Захват вычислительных ресурсов
- Недоброжелатели
- Идеологические противники
- Just for fun



ВИДЫ АТАКУЮЩИХ

- Роботы (ботнеты)
- Профи

- White Hat Hacker

- Black Hat Hacker

- Grey Hat Hacker

- Script kiddie / Newbie
- Criminal gangs — криминальные группы
- Hacktivist — хактивисты, идеологические противники
- Cyberwarfare — кибер-войска

НАПРАВЛЕННЫЕ АТАКИ

- Сложные и стойкие угрозы (advanced persistent threats, APT)

ВЫДЕРЖКА ИЗ ОТЧЁТА RSA EMC “WHEN ADVANCED PERSISTENT THREATS GO MAINSTREAM”

	Обычные угрозы	Сложные и стойкие угрозы
Кто инициатор атак?	Корыстолюбивые хакеры и киберпреступники	Хорошо финансируемые и подготовленные противники: политические враги, недобросовестные конкуренты, глобально организованная преступность
Какие данные являются целью и мишенью атак?	Данные кредитных карт и банковских учетных записей, персональные данные, любая информация, интересная многочисленному кругу покупателей	Интеллектуальная собственность; данные, касающиеся обеспечения национальной безопасности; коммерческая тайна; исходные коды программ; данные исследований и разработок; финансовая информация; производственные и бизнес-планы; другие сведения, интересные относительно узкому кругу покупателей
Какие организации являются мишенью?	Любое предприятие и целые отрасли, особенно финансовый сектор	Конкретная организация, главным образом, правительственные, оборонные, энергетические, финансовые и высокотехнологичные предприятия
Цель атак	Доход (нелегальный), кражи личности, мошенничество, самовыражение	Влияние на рынок; достижение конкурентного преимущества; влияние на национальную обороноспособность; занятие выгодной позиции на переговорах; повреждение критически важной инфраструктуры противника и т.д.
Методы атак	Главным образом – атаки на периметр сети предприятия	Основным методом являются атаки через пользователей (социальная инженерия и целевой фишинг), а также через конечные устройства (эксплуатация уязвимостей программ и другие способы). Атаки часто характеризуются сложностью и многоступенчатостью

КОМПЬЮТЕРНЫЕ ВИРУСЫ

- Компьютерные вирусы - разновидность вредоносных программ, отличительной особенностью которых является способность к размножению (саморепликации).

КЛАССИФИКАЦИЯ ВИРУСОВ

- По поражаемым объектам: файловые вирусы, загрузочные вирусы, скриптовые вирусы, сетевые черви.
- По поражаемым операционным системам и платформам: DOS, Microsoft Windows, Unix (Linux, Android)
- По технологиям используемым вирусом: полиморфные вирусы, стелс-вирусы
- По языку, на котором написан вирус: ассемблер, высокоуровневый язык программирования, язык сценариев.
- По механизму заражения: паразитирующие, перезаписывающие, спутники
- По дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.)

УЯЗВИМОСТЬ

- Уязвимость - это недостаток программно-технического средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации.
- Уязвимость – это слабое место актива или средства контроля и управления, которое может быть использовано злоумышленниками.

КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ

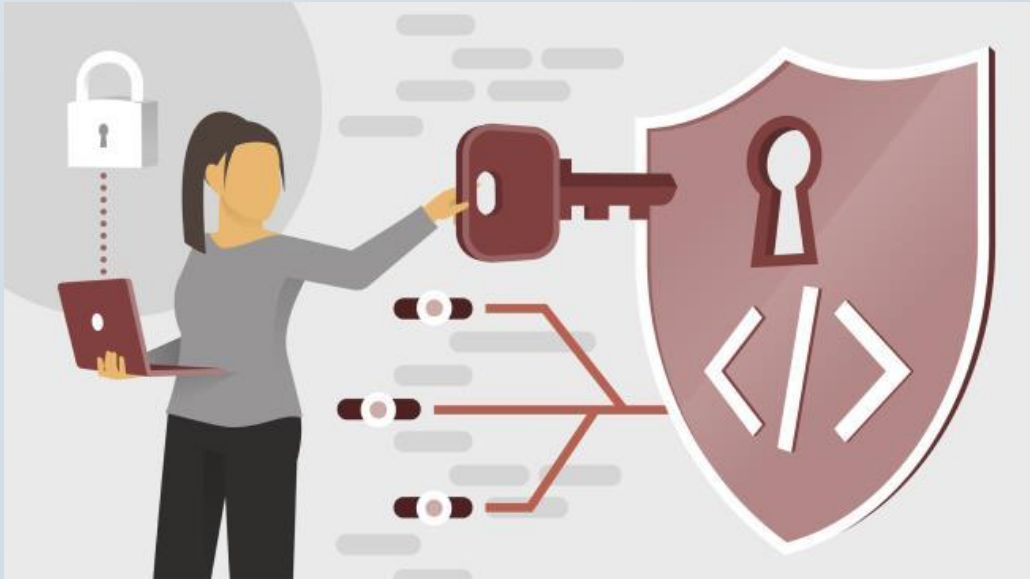
- объективными;
- случайными;
- субъективными.

ТИПЫ УЯЗВИМОСТЕЙ

- уязвимость кода (баги, логические ошибки и т.д);
- уязвимость конфигурации;
- уязвимость архитектуры;
- организационная уязвимость;
- многофакторная уязвимость.

БЕЗОПАСНОЕ ПРОГРАММИРОВАНИЕ

- Методика разработки программного обеспечения, предотвращающая случайное внедрение уязвимостей и обеспечивающая устойчивость к воздействию вредоносных программ и несанкционированному доступу.
- Defensive programming (Оборонительное, защитное, безопасное программирование)
- Secure coding (Безопасное программирование)



DEFENSIVE PROGRAMMING

- Оборонительное, защитное, безопасное программирование — принцип разработки ПО, при котором разработчики пытаются учесть все возможные ошибки и сбои, максимально изолировать их и при возможности восстановить работоспособность программы в случае неполадок.

SECURE CODING

Безопасное программирование — методика написания программ, устойчивых к атакам со стороны вредоносных программ и злоумышленников.

БЕЗОПАСНОЕ ПО

Программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы

НЕБЕЗОПАСНАЯ ПРОГРАММА

Потенциальная цель для злоумышленника, которыий может использовать имеющиеся уязвимости для просмотра, изменения или удаления имеющейся информации, влияния на работу программ и сервисов (запуск или остановка), внедрения вредоносного кода в систему