Государственное бюджетное
профессиональное образовательное
учреждение города Москвы
«КОЛЛЕДЖ ПОЛИЦИИ»

Информатика и информационные технологии в профессиональной деятельности
Угрозы информационной безопасности.
Классификация угроз информационной безопасности

Выполнил курсант 211 взвода
Бакаева Анастасия Равшановна
Преподаватель
Тарас Ольга Борисовна

Постановка проблемы, актуальность и новизна

Актуальность

- Угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты

Проблема

- Независимо от того, что лежит в основе воздействия: естественные факторы или причины искусственного характера – владелец информации несет убытки.

Новизна

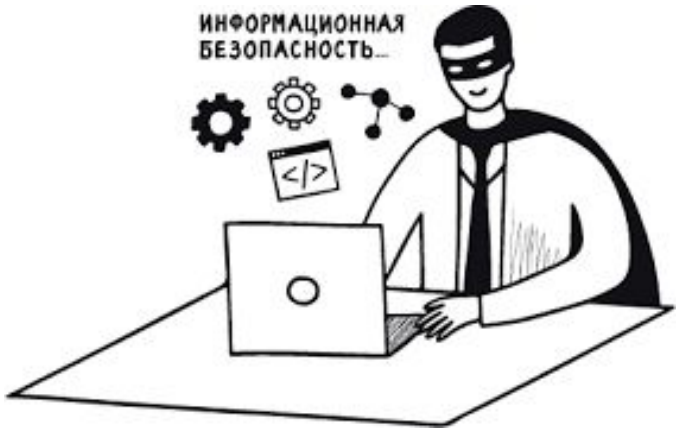
- противодействие идеологии терроризма, информационная сфера, информационные угрозы, информационная безопасность, защита информационно-психологических угроз.

Цели и задачи работы

Цель: Раскрыть тему информационной угрозы

Задачи:

- ликвидации угроз объектам информационной безопасности;
- минимизация возможного ущерба, который может быть нанесен вследствие реализации данных угроз;
- рассчитать процент внешней и внутренней угроз.



Основные определения

Информационная безопасность	Атака	Злоумышленник	Окно опасности	Угроза
• это защищенность информационной среды личности, общества и государства от преднамеренных и непреднамеренных угроз и воздействий	• это массовая атака хакеров (одного или группы людей, которые незаконно проникают в чужие аккаунты или учетные записи), когда могут пострадать очень много почтовых ящиков, электронных кошельков, банковских карт или других ресурсов интернета обычных пользователей.	• человек, который предпринимает попытку атаки	• промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется.	• это потенциальная возможность определенным образом нарушить ИБ

Классификация угроз информационной безопасности

Расположение источника
- Внутренние
- Внешние

По характеру ущерба
- материальные
- моральные

По объектам
- персонал
- финансы
- информация
- материальные ценности

По характеру воздействия
- активные
- пассивные

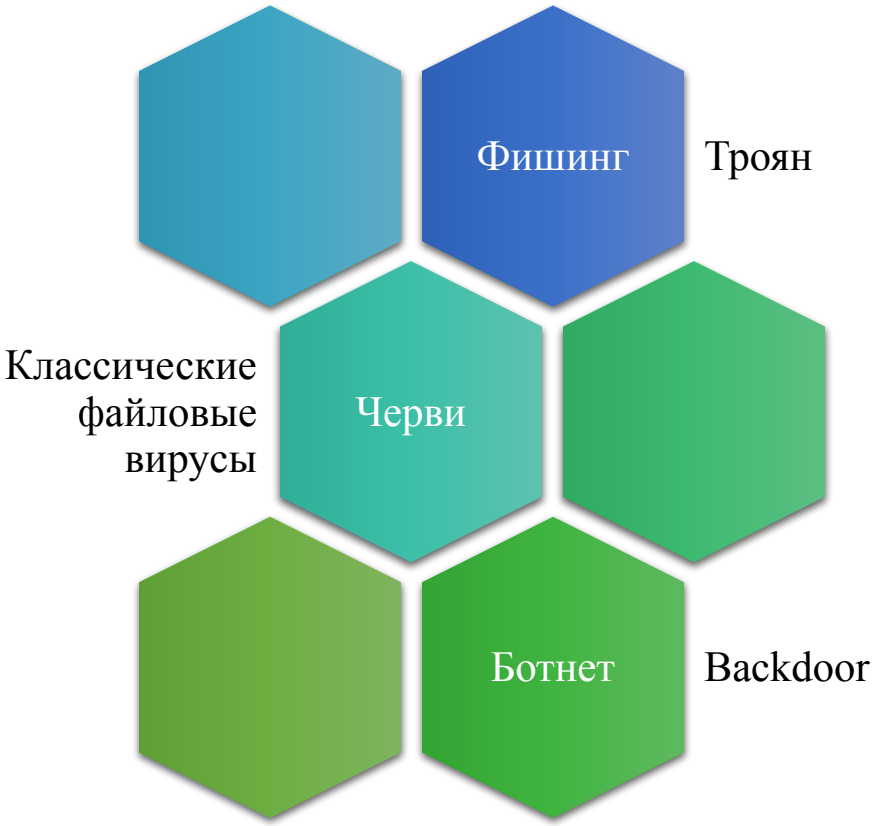
По величине ущерба
- предельный
- значительный
- незначительный

По аспекту информационной безопасности: доступность, целостность, конфиденциальность, против которого угрозы направлены в первую очередь

Жертвы информационных угроз

Государство	Компания (юридическое лицо)	Личность (физическое лицо)
• Информационная война • Информационные противодействия • Информационное оружие, кибератаки	•Разглашение •Утечка •Несанкционированный доступ	•Киберслежка •Онлайновое мошенничество (поддельные письма) •Фишинг (раскрытие персональных данных: логина, пароля, номера банковской карты)

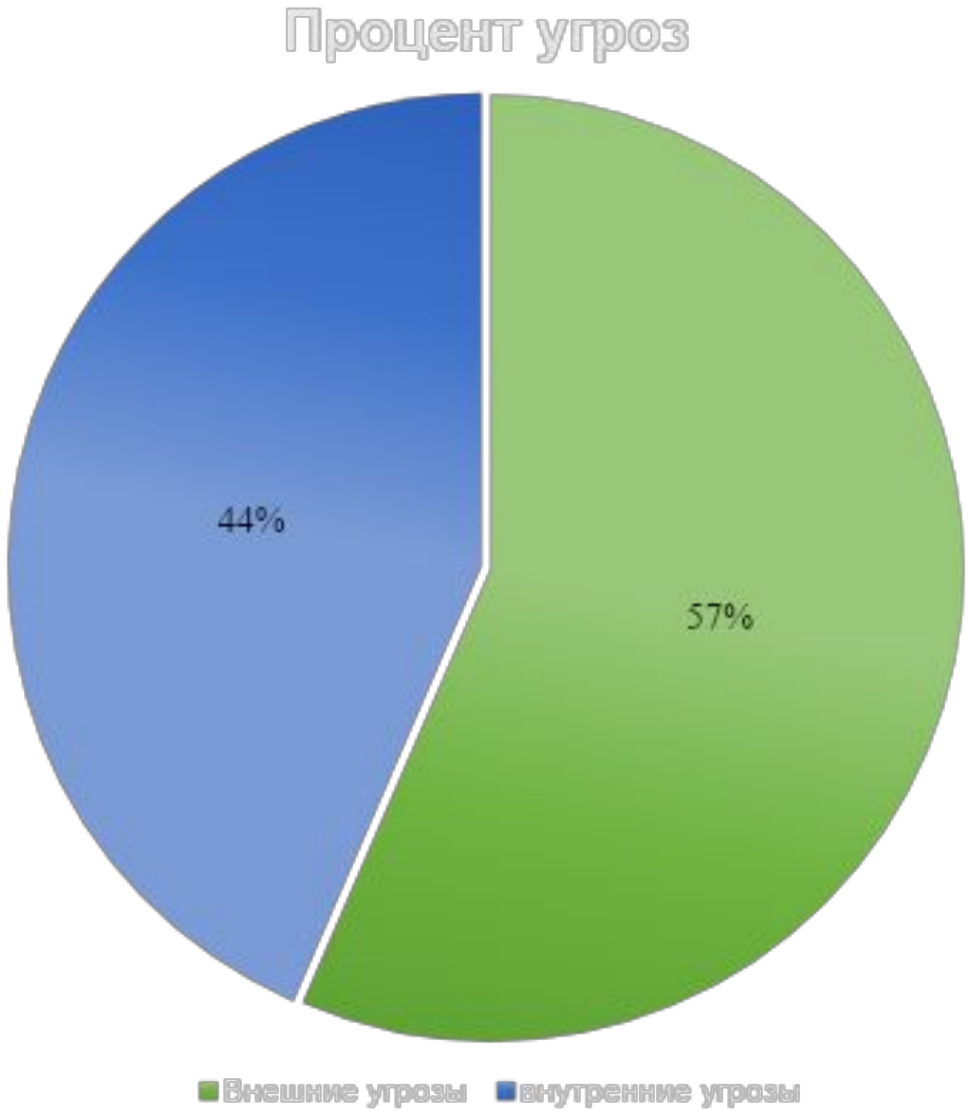
Наиболее опасные угрозы ИБ



Внешние и внутренние угрозы

Внутренние: ошибки пользователей и сисадминов; ошибки в работе ПО; сбои в работе компьютерного оборудования; нарушение сотрудниками компании регламентов по работе с информацией.

Внешние угрозы: несанкционированный доступ к информации со стороны заинтересованных организаций и отдельных лица (промышленный шпионаж конкурентов, сбор информации спецслужбами, атаки хакеров и т. п.); компьютерные вирусы и иные вредоносные программы; стихийные бедствия и техногенные катастрофы (например, ураган может нарушить работу телекоммуникационной сети, а пожар уничтожить сервера с важной и ценной информацией).



Угрозы по характеру воздействия и их причины

Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например:

- недовольством служащего служебным положением;
- любопытством;
- конкурентной борьбой;
- уязвленным самолюбием и т. д.

Свойства угроз

Избирательность	нацеленность угрозы на нанесение вреда тем или иным конкретным свойствам объекта безопасности
Предсказуемость	наличие признаков возникновения, позволяющих прогнозировать возможность появления угрозы и определять конкретные объекты безопасности, на которые она будет направлена
Вредоносность	возможность нанесения вреда различной тяжести объекту безопасности

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Основной способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль.

Основные типы угроз информационной безопасности

Угрозы конфиденциальности – несанкционированный доступ к данным (например, получение посторонними лицами сведений о состоянии счетов клиентов банка).

Угрозы целостности – несанкционированная модификация, дополнение или уничтожение данных (например, внесение изменений в бухгалтерские проводки с целью хищения денежных средств).

Угрозы доступности – ограничение или блокирование доступа к данным (например, невозможность подключится к серверу с базой данных в результате DDoS-атаки).

Виды угроз информационной безопасности

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

- неправомерное включение оборудования или изменение режимов работы устройств и программ;

- неумышленная, порча носителей информации;

- Запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

- заражение компьютера вирусами;

«Вредительские программы»- угроза безопасности

Вирус – это искусственная компьютерная программа или часть кода, который вызывает неожиданные, как правило, отрицательные, последствия выполненные программным путем на вашем компьютере. Вирусы часто **маскируются под игры** или изображения с красивыми известными брендами или названиями;

«Троянские кони», Trojan – вредоносная программа, которая претендует на доброкачественное приложение; программа-троян целенаправленно делает, то, что пользователь совсем не ожидает или не хочет делать. Трояны не являются вирусами, так как они не размножаются, но эти программы могут быть столь же разрушительны как и вирусы.

СПАМ (S.P.A.M. – в переводе с англ. «обрезки, куски, остатки») является нежелательным получением любых электронных сообщений. Существует СПАМ в электронной почте, на сайтах, в баннерах, в новостях, СПАМ веб-поиске, СПАП в блогах, и мобильный спам по SMS. СПАМ это реклама, вводящая в заблуждение пользователя;

Программы-шпионы имеют широкий спектр деятельности, в основном это нежелательные программы, которые используют зараженные компьютеры для получения коммерческой выгоды. Они могут доставить нежелательные всплывающие окна с рекламой, украсть личную информацию (включая финансовую информацию, такую как номера кредитных карт), контролировать веб-страницы для деятельности в маркетинговых целях.

Средства защиты информации

•Организационные. Комплекс мер и средств организационно-правового и организационно-технического характера. К первым относят законодательные и нормативные акты, локальные нормативные документы организации. Второй тип — это меры по обслуживанию информационной инфраструктуры объекта.

•Аппаратные (технические). Специальное оборудование и устройство, предотвращающее утечки, защищающее от проникновения в ИТ-инфраструктуру.

•Программные. Специальное ПО, предназначенное для защиты, контроля, хранения информации.

•Программно-аппаратные. Специальное оборудование с установленным программным обеспечением для защиты данных.

Каналы несанкционированного доступа к информации

Через человека:	Через программу:	Через аппаратуру:
• хищение носителей информации; • чтение информации с экрана или клавиатуры; • чтение информации из распечатки.	• перехват паролей; • расшифровка зашифрованной информации • копирование информации с носителя	• подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации; • перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания

Типы программных средств защиты:

- Антивирусное ПО.
- Облачные антивирусы (CloudAV).
- Решения DLP (Data Leak Prevention).
- Системы криптографии. (DES — Data Encryption Standard, AES — Advanced Encryption Standard).
- Межсетевые экраны (МСЭ)
- Виртуальные частные сети VPN (Virtual Private Network). Прокси-сервер.

Инструменты для защиты информации

Физические

- Это инструменты, которые существуют в физическом мире. К ним обычно относится различное оборудование. Пластиковые ключи-карты и замки, которые открываются по ним, — это физический инструмент. Установленные в дата-центре резервные сервера — тоже. Еще сюда можно отнести видеонаблюдение и сигнализацию, использование сейфов, работу с физическими источниками информации, мониторинг оборудования и многое другое.

Технические и программные

- Это то, что относится скорее к софту, а не к железу, от защищенных протоколов до антивируса. Шифрование данных, передача сведений через HTTPS, установка брандмауэра и так далее — такие меры. Есть и специальные инструменты: защитное ПО и сервисы, программы для поиска уязвимостей и имитации атак, многое другое. К техническим средствам еще можно отнести построение инфраструктуры защищенной системы и сети.
- Некоторые компании называют техническими средствами все, что связано с техникой. Это ярко видно, например, в официальных документах, даже если фактически они описывают физические методы.

Угрозы информационной безопасности России

По результатам исследования «Лаборатории Касперского» 36% российских пользователей минимум один раз пострадали от взлома аккаунта, в результате чего были украдены их персональные данные, либо профиль был использован для рассылки вредоносного ПО.

Чаще всего злоумышленников интересует доступ к аккаунту в социальной сети и электронной почте (14%) и пароль к онлайн-банкингу (5%).

53% респондентов в результате взлома получили фишинговые сообщения или попали на подозрительные сайты, целью которых было вытягивание из них учетных данных. Информация, хранившаяся в профиле, была полностью уничтожена у каждой пятой жертвы, а в 14% случаев персональные данные были использованы в преступных целях, например, для проведения несанкционированных транзакций.

Страдают от действий киберпреступников не только сами пользователи, чьи учетные данные были украдены, но также их друзья и родственники. Так, более половины жертв взлома аккаунта обнаружили, что кто-то рассылал сообщения от их имени, и почти каждый четвертый - что их друзья кликнули на полученную от них вредоносную ссылку.

Несмотря на это, только 28% пользователей создают надежные пароли для своих аккаунтов и только 25% выбирают безопасные способы их хранения.

kaspersky

Подведение итогов

Жизнь современного общества немыслима без современных информационных технологий; в свою очередь высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т. п.).

Несанкционированный доступ является одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющим нанести ущерб любой из составляющих информационной безопасности.

Угрозы информационной безопасности классифицируются по нескольким признакам:

· по характеру воздействия;

· по расположению источника угроз.

Приведенные примеры нарушения личной и государственной информационной безопасности в очередной раз доказывают, что существующими угрозами ни в коем случае нельзя пренебрегать ни самим пользователям сети Интернет, ни организациям и предприятиям.