



ОСНОВНЫЕ ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДЫ ИХ ВЫЯВЛЕНИЯ

Столбов Павел Андреевич

студент, Сочинский государственный университет
РФ, г. Сочи

Аннотация. В статье рассмотрены вопросы информационной безопасности в России. Проанализированы основные источники угроз информационной безопасности, а также средства защиты от таких угроз.

Ключевые слова: информационная безопасность, источники угрозы, харек, кибербезопасность, взлом.

Анализ отчета InfoWatch за 2023 год демонстрирует неоднозначную динамику в сфере информационной безопасности. С одной стороны, на глобальном уровне наблюдается некоторое снижение числа утечек данных: 1773 случая за первые 9 месяцев 2023 года против 1916 случаев за аналогичный период 2022 года, что составляет спад на 7,4%. Объем скомпрометированных данных также сократился на 1,4%, составив 9,93 млрд записей.

Однако эта позитивная тенденция не распространяется на Россию, где, напротив, зафиксирован рост числа утечек на 5,6% (302 случая в 2023 году против 286 случаев в 2022 году).

Выделяют следующие основные источники угроз, не считая хакерских атак. К ним относятся:

1. Человеческий фактор: Невнимательность и неосторожность сотрудников — одна из наиболее распространенных причин утечек. Открытие фишинговых писем, использование инфицированных носителей информации — все это может привести к серьезным последствиям для организации.
2. Использование нелегального ПО: Пиратское ПО не получает своевременных обновлений безопасности, что делает его уязвимым для атак. Исследования Microsoft показывают, что около 7% нелегальных программ содержат вредоносное ПО.

3. Внутренние нарушители: сотрудники организации, имеющие легальный доступ к информационным ресурсам и злоупотребляющие своими полномочиями (умышленно или по неосторожности). К ним относятся:

- Злоумышленники («кроты»): сотрудничают с конкурентами или другими третьими лицами на возмездной основе или руководствуясь корыстными побуждениями.
- нелояльные сотрудники («уволенные»): похищают конфиденциальную информацию при увольнении.
- Недобросовестные руководители: злоупотребляют служебным положением для получения доступа к закрытой информации.
- Невнимательные сотрудники: становятся причиной утечек из-за нарушения правил работы с информацией и несоблюдения требований ИБ.

4. Государственные органы: в рамках законодательства могут изымать электронные носители информации, что способно привести к простоям в работе и финансовым потерям для организации.

5. Атаки на доступность. DDoS-атаки: перегружают ресурс трафиком, выводя его из строя, часто используются против банков

Существует, также и иные, более общая классификация всех возможных угроз информационной безопасности. В ней угрозы могут разделяться по разным классификационным признакам:

1. По источнику возникновения:

Объективные угрозы (естественные): вызваны объективными факторами, не зависящими от воли человека. К ним относятся стихийные бедствия (пожары, наводнения, землетрясения), аварии на объектах инфраструктуры (отключение электроэнергии, связи), воздействие агрессивных сред.

Субъективные угрозы (искусственные): являются результатом целенаправленных или случайных действий человека. Данная группа угроз включает в себя как умышленные действия злоумышленников (хакеров, конкурентов, террористов), так и ошибки, допущенные сотрудниками организации (случайное удаление данных, нарушение правил работы с конфиденциальной информацией).

2. По направленности действий:

Угрозы конфиденциальности: нарушение установленного режима доступа к информации и ее разглашение неавторизованным лицам.

Угрозы целостности: несанкционированное изменение информации, ее искажение или уничтожение.

Угрозы доступности: нарушение своевременного и гарантированного доступа к информационным ресурсам и сервисам.

3. По характеру воздействия:

Пассивные угрозы: направлены на несанкционированное получение информации без внесения изменений в работу информационной системы (например, перехват данных, передаваемых по сети).

Активные угрозы: предполагают осуществление каких-либо действий, направленных на нарушение работы информационной системы, модификацию или уничтожение данных (например, вирусные атаки, внедрение вредоносного кода, DDoS-атаки).

4. По степени преднамеренности:

Случайные угрозы: возникают в результате ошибок персонала, сбоев в работе оборудования, непредвиденных ситуаций (например, случайное удаление важного файла, выход из строя жесткого диска).

Преднамеренные угрозы: являются результатом осознанных и спланированных действий злоумышленников, направленных на достижение конкретных целей (например, хищение конфиденциальных данных, вывод из строя информационной системы, шантаж).

5. По локализации источника угрозы:

Внешние угрозы: исходят от субъектов, находящихся вне периметра защиты информационной системы организации (например, атаки хакеров из сети Интернет, действия конкурентов, проникновение вредоносного ПО из внешних источников).

Внутренние угрозы: связаны с действиями сотрудников организации (как умышленных, так и непреднамеренных), а также с использованием внутренних ресурсов организации в злоумышленных целях (например, хищение данных нелояльным сотрудником, нарушение политик безопасности по неосторожности).

6. По способу доступа к информации:

Угрозы с прямым доступом: реализуются путем непосредственного физического или логического доступа к информационным ресурсам (например, кража ноутбука с конфиденциальными данными, несанкционированный доступ к базе данных с использованием уязвимости в системе защиты).

Угрозы со скрытым доступом: реализуются без явного нарушения периметра безопасности, с использованием вредоносного ПО или методов социальной инженерии (например, заражение компьютера вирусом, фишинг).