**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра прикладной экономики**

ЭССЕ

**по дисциплине «Экономика»**

**по теме:** Проблема цифровой безопасности предпринимательских структур

|  |  |  |
| --- | --- | --- |
| Студент гр. 3584 |  | Шеин П.О. |

Преподаватель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Олехова Н.И.

Санкт-Петербург

2025

# 2)Введение:

Цифровые угрозы растут с каждым годом. Только в 2023 году ущерб от

кибератак в мире составил более $8 млрд. При этом 60% малых компаний

после серьезной утечки данных закрываются в течение полугода.

Кибербезопасность – это набор процессов и стратегий для защиты критически важных систем и конфиденциальной информации компании от кибератак и утечек данных. Приемы злоумышленников становятся все более изощренными по мере увеличения ландшафта угроз, и для разработки новых методов киберпреступники используют искусственный интеллект и социальную инженерию. И чтобы не отставать от них, бизнесу приходится постоянно укреплять защиту.

# Основные угрозы:

**Извне — хакеры, вирусы, фишинг;**

Существует несколько разновидностей кибератак, нацеленных на кражу конфиденциальных сведений или вывод из строя внутренних систем, устройств:

Одной из наиболее распространенных внешних угроз являются кибератаки, которые включают в себя фишинг, DDoS-атаки, внедрение вредоносного программного обеспечения и целевые атаки. Хакеры могут использовать уязвимости в системах безопасности для получения

несанкционированного доступа к конфиденциальной информации, шпионажа или саботажа. Особенно опасными являются целевые атаки, направленные на конкретные компании с целью похищения интеллектуальной собственности или финансовых данных.

Фишинг - рассылка мошенниками писем с целью получить личные данные адресата или развернуть вредоносное ПО на устройстве или в сети жертвы.

DoS — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.

Чаще всего похищается информация следующих типов:

* общедоступная внутренняя операционная информация;
* персональные данные клиентов;
* базы данных клиентов компании;
* закрытая финансовая информация, управленческая отчетность;
* интеллектуальная собственность;
* маркетинговые исследования, исследования о конкурентах;
* платежная информация, данные о банковских транзакциях.
  + Социальная инженерия. Это метод манипулирования людьми с целью заставить их предоставить конфиденциальную информацию или выполнить определенные действия, которые могут нанести ущерб безопасности предприятия. Социальные инженеры могут использовать различные методы, такие как звонки от имени представителей банка или IT-отдела, чтобы обмануть сотрудников и получить доступ к конфиденциальной информации.
  + Физическое воздействие. Например, злоумышленник может повредить серверы, хранящие конфиденциальные данные, или похитить оборудование, содержащее важную информацию. Физическое воздействие может привести к прекращению работы предприятия на длительный срок, что может нанести ущерб репутации компании и привести к финансовым потерям.

# Изнутри — ошибки сотрудников или даже умышленный вред;

Внутренние угрозы информационной безопасности представляют собой серьезную опасность для предприятий любого размера и профиля. Они могут исходить от сотрудников, партнеров или других лиц, имеющих доступ к внутренним системам и данным. Рассмотрим основные виды таких угроз и способы их минимизации.

* + Утечка данных по неосторожности. В этом случае угрозы информационной безопасности предприятий возникают из-за банальной невнимательности или влияния человеческого фактора. Например, сотрудник может случайно перепутать адресата в электронной почте и не туда отправить важные сведения. Или перейти по сомнительной ссылке, тем самым скомпрометировав учетные и персональные данные.
  + Злонамеренные действия сотрудников. Может проявляться в различных формах, таких как кража информации, саботаж, мошенничество, шпионаж, несанкционированный доступ к конфиденциальным данным или даже физическое повреждение имущества компании. Такое поведение может нанести серьезный ущерб безопасности и стабильности организации.

1. Ущерб бывает:

* **Фактическим**, в виде прпавших денег со счетов, сумм, выплаченных вымогателям, заразившим систему вирусами, ущерба от приостановки бизнес- процессов. Особой статьей расходов становятся штрафы, выплаченные в

бюджет, и ущерб, компенсированный клиентам в результате выигранных процессов в связи с утратой компанией ценной информации;

* **Расчетным**, когда суммы неполученной прибыли от утечки ценной информации можно рассчитать исходя из финансовых показателей деятельности компании и из сумм, потраченных на спешное обновление системы информационной безопасности;
* **Репутационным** – компания теряет рынки, клиентов, стоимость ее акций падает в ситуации, когда становится известно о ее неосмотрительном поведении и недостаточной защите важных данных.

Ущерб может проявиться лишь спустя длительное время, например, когда ноу-хау было похищено инсайдером и появилось в распоряжении конкурентов через годы.

**5) Некоторые меры, которые помогают решить проблему цифровой безопасности:**

* Организационные

Делятся на две группы. Организационно-технические: подготовка помещений с компьютерами, прокладка кабельной системы с учётом требований ограничения доступа к ней. И организационно-правовые: национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия.

1. • Аппаратные

Механические, электромеханические и электронные устройства, которые решают задачи безопасности на уровне оборудования. Чаще всего используются для защиты помещений от прослушивания и предотвращения несанкционированного доступа к данным. К ним относятся генераторы шума, сетевые фильтры, сканирующие радиоприёмники и др. Аппаратные средства необходимы, чтобы выстроить несколько уровней защиты информации.

* + Программные

Программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Далее в статье эти средства описаны более подробно.

1. Из программного обеспечения можно использовать:
   * Антивирусное ПО.
   * Облачные антивирусы (CloudAV). К таким решениям относятся сервисы Panda Cloud Antivirus, Immunet и многие другие. Облачные антивирусы идеально

подходят для защиты ПК, у которых нет достаточной вычислительной мощности.

* + Специальные программы, предотвращающие утечку данных (Data Leak Prevention). Внедрение и поддержка DLP требуют достаточно больших вложений и усилий со стороны предприятия. Однако эта мера способна значительно уменьшить уровень информационных рисков для IT- инфраструктуры компании.
  + Системы криптографии (DES — Data Encryption Standard, AES — Advanced Encryption Standard).
  + Межсетевые экраны (МСЭ). Они обеспечивают фильтрацию и блокировку нежелательного трафика, контролируют доступ в сеть. Различают такие виды фаерволов, как сетевые и хост-серверы.
  + Виртуальные частные сети VPN (Virtual Private Network). Решение, использующее в рамках общедоступной сети частную сеть для передачи и приёма данных, что даёт эффективную защиту подключённых к сети приложений.
  + Прокси-сервер. Выполняет функцию шлюза между компьютером и внешним сервером.
  + Решения SIEM — системы мониторинга и управления информационной безопасностью. SIEM собирает сведения о событиях из всех источников, поддерживающих безопасность, в том числе от антивирусного ПО, IPS, фаерволов, а также от операционных систем и т.д.

**8) Заключение**

Обеспечение информационной безопасности сегодня является одной из главных потребностей, пренебрежение которой может иметь разрушительные последствия для бизнеса. Выбор инструментов защиты информации должен зависеть от сферы деятельности, размера и технической оснащённости компании, уровня подготовки и опыта сотрудников.

**СПИСОК ИСПОЛЬЗУЕ МОЙ ЛИТЕРАТУРЫ**

1) Информационная безопасность предприятий: средства и способы ее обеспечения.[Электронный ресурс]. URL: https://rt-solar.ru/products/solar\_dozor/blog/4492/

2) kaspersky – Почему малый бизнес должен серьезно относиться к кибербезопасности [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/small-business-security

3) Информационная безопасность: как защитить бизнес. [Электронный ресурс]. URL: https://kdelu.vtb.ru/articles/informaczionnaya-bezopasnost-kak-zashhitit-biznes/