



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФОРМА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Суслов Владислав Андреевич

студент

научный руководитель: Валько Данила Валерьевич

к.э.н., доцент

ОУ ВО «Южно-Уральский технологический университет», г. Челябинск

Аннотация. Новые реалии современности требуют нового подхода к вопросам обеспечения экономической безопасности, в которой все более важную роль начинают играть информационная безопасность. Такие тенденции интенсивно развиваются с 80-х гг. в прошлого века и вызваны научно-техническим прогрессом в сфере информационных технологий, глобальных систем телекоммуникаций, средств связи. В указанном периоде возникли эффективные технические средства цифрового информационного обмена, которые могли обеспечивать информационно-телекоммуникационное соединение различных районов мира в глобальную экономическую систему.

Ключевые слова: Информационная безопасность, правовое обеспечение, киберпространство, государственная политика, конфиденциальные данные.

Информационная безопасность- это защищенность информации от незаконного получения, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Источниками этих воздействий могут быть проникновение злоумышленников, ошибки персонала, выход из строя аппаратных и программных средств, стихийные бедствия (землетрясение, ураган, пожар и т. п.).

Защита информации - это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Цели защиты информации:

- целостность данных;
- конфиденциальность данных;
- доступность данных.

Целостность данных гарантирует, что они не были изменены, подменены или уничтожены в результате злонамеренных действий или случайностей. Обеспечение целостности данных - одна из самых сложных задач защиты информации.



Конфиденциальность данных - это статус, предоставленный данным и определяющий требуемую степень их защиты. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизацию) субъектам информационной системы (пользователям, процессам, программам). Примеры конфиденциальных данных:

- личная информация пользователей;
- учетные записи (имена и пароли);
- данные о кредитных картах;
- бухгалтерские сведения.

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы ИБ РФ и методы ее обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения ИБ, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз ИБ РФ. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения ИБ РФ могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние ИБ РФ.

Обеспечение ИБ РФ в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Воздействию угроз ИБ РФ в сфере экономики наиболее подвержены:

1. система государственной статистики;
2. кредитно-финансовая система;
3. информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;
4. системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;
5. системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

РАСПРЕДЕЛЕНИЕ ИБ-ИНЦИДЕНТОВ В ЧЕТВЕРТОМ КВАРТАЛЕ 2022 ГОДА ПО КАТЕГОРИЯМ (%)

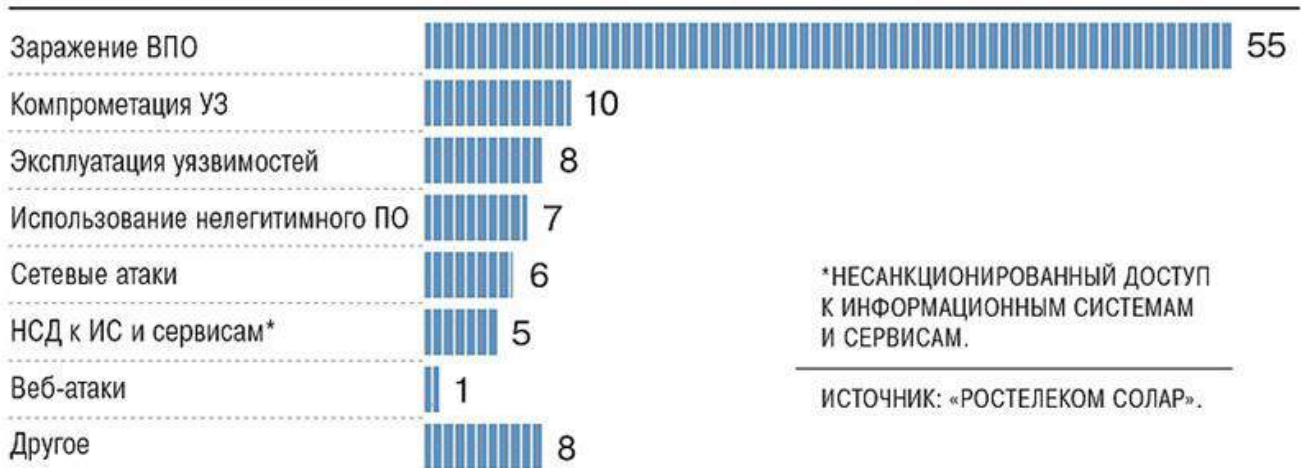


Рисунок 1 – Распределение ИБ-инцидентов в четвёртом квартале 2022 года по категориям (%)

В 2022 году на российские компании было совершено 911 тыс. хакерских атак, что вдвое больше, чем годом ранее. Такие данные «Ростелеком-Солар» обнародовал 20 февраля 2023 года.

Исследование экспертов охватывает 280 организаций из разных отраслей, включая госсектор, финансы, энергетику, телеком, медиа, крупный ритейл. Данная статистика не включает массовые DDoS-атаки.

По словам ИБ-специалистов, на фоне общего роста атак во втором полугодии снизилось их число со стороны хактивистов — непрофессиональных хакеров, действующих по политическим, а не коммерческим мотивам с применением простых инструментов, например массовых DDoS-атак или атак на веб-серверы. Например, если в первом полугодии доля нападений хактивистов на веб-серверы в России составляла 11% от всех инцидентов, то во второй половине 2022 года — только 1%.

В исследовании говорится, что к концу 2022 году в России увеличилось число сетевых атак. Зачастую сканирование периметра или веба и попытки компрометации учетных записей выполняются автоматизированными инструментами, которые хакеры используют для разведки в отношении клиента. Несмотря на низкий уровень критичности таких инцидентов, это опасный звонок для компаний, который указывает на то, что они привлекательны для злоумышленников. А значит, им необходимо продолжать тренд на усиление своей киберзащиты, заявили в «Ростелеком-Солар».

Выросло число кибератак на ИТ-компании через шпионское ПО

Количество кибератак на российские ИТ-компании в четвертом квартале 2022 года увеличилось на 18% в сравнении с тремя предыдущими месяцами. При этом в 62% случаев хакеры использовали вредоносное программное обеспечение, преимущественно программы шифровальщиков, направленные на кражу конфиденциальной информации и получение выкупа. Об этом говорится в исследовании, которое Positive Technologies опубликовала 17 февраля 2023 года.

Эксперты отметили долю атак с использованием шпионского ПО: в октябре-декабре 2022 года 17% таких атак было совершено в отношении организаций, 49% — в отношении частных лиц; это на соответственно 5 п. п. и 3 п. п. больше показателей третьей четверти 2022 года. Злоумышленники создают новые вредоносы и работают над расширением их функциональности: так, в новом стилере Augora появилась функция кражи данных не только из браузеров или буфера обмена, но и непосредственно с диска устройства.

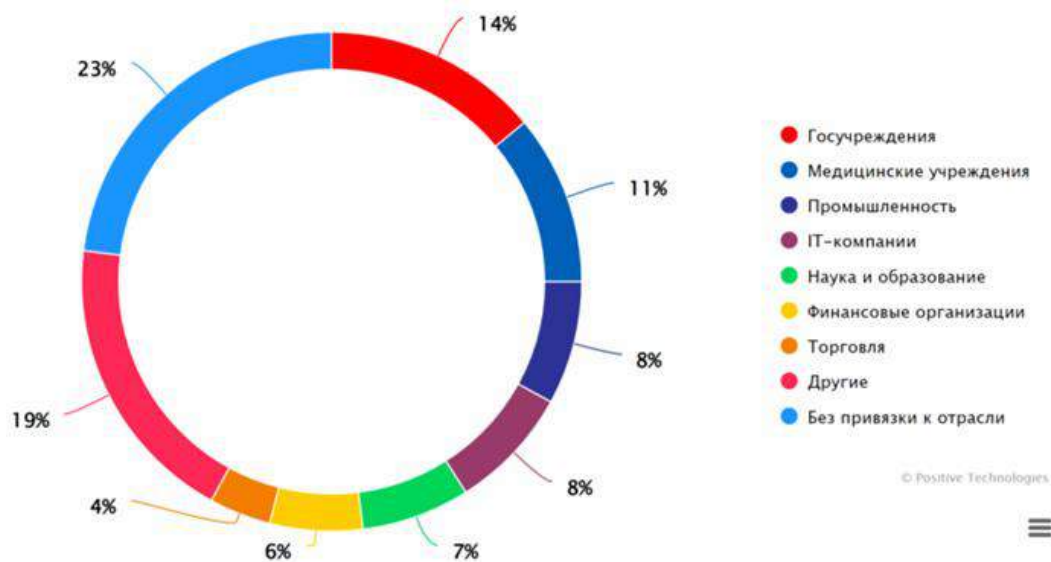


Рисунок 2 – Категории жертв среди организаций

Распространение вирусов-шпионов по схеме «вредонос как услуга» позволяет использовать их даже неопытным злоумышленникам: исследователи Positive Technologies проанализировали новый стилер BlueFox, который активно продвигается на подпольном рынке по такой схеме. Кроме того, участились случаи встраивания вредоносного кода, который выполняет функции шпионского ПО, в пакеты для разработчиков Python — это может привести к росту числа атак типа supplychain. Кибератака, в ходе которой злоумышленники взламывают компанию путем компрометации поставщиков ПО или оборудования. Например, преступники могут внедрить вредоносный код в исходный код продукта или распространить вредоносные



обновления, чтобы заразить инфраструктуру целевой организации. и компрометации сетей ИТ-компаний.

Список литературы:

1. Косовец А.А. Вестник Академии экономической безопасности МВД России: учеб.пособие для вузов., 2011 – 20-25 с.
2. Информационная безопасность и защита информации
Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. – 7-8 с.
3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2023. 80-93 с.
4. Ростелеком-Солар. Корпоративная безопасность - https://rt-solar.ru/products/solar_dozor/blog/3335/
5. PositiveTechnologies — российская компания, специализирующаяся на разработке решений в сфере информационной безопасности. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2022-q2/?sphrase_id=155486