Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

«Санкт-Петербургский политехнический университет Петра Великого»

Институт компьютерных наук и технологий

Высшая школа интеллектуальных систем и суперкомпьютерных технологий

**Реферат**

**Тема: Анализ основных <OPPONENT> информационной безопасности**

**Дисциплина**: «Защита информации»

Выполнил студент гр. 3530901/80202

Чернышев Ярослав Николаевич

Преподаватель

Новопашенный Андрей Гелиевич

Санкт-Петербург

2022

Содержание

[Содержание 2](#_Toc97022998)

[Введение 3](#_Toc97022999)

[1. Атаки на отдельных лиц 4](#_Toc97023000)

[2. Атаки на организации 5](#_Toc97023001)

[3. Криптовалюты 9](#_Toc97023002)

[4. Интернет вещей 10](#_Toc97023003)

[Выводы 11](#_Toc97023004)

[Список использованных источников 12](#_Toc97023005)

# Введение

По состоянию на начало 2022 года можно с уверенностью сказать, что набирает обороты четвёртая промышленная революция. Она обычно описывается путем указания ключевых технологий, которые «скоро» будут внедрены в быт человека. К данным технологиям, для примера, можно причислить следующие инновации, которые уже входят в жизнь:

* Аналитика больших данных
* Квантовые вычисления
* «Интернет вещей»
* Дополненная и виртуальная реальности
* Трёхмерная печать
* Криптовалюты

И многие другие

Любой технологический скачок влечёт за собой и изменения в сопутствующих областях, как положительные, так и отрицательные. Информационные технологии являются одной из самых быстроразвивающихся отраслей, и именно поэтому вопрос безопасности – информационной безопасности – стоит особенно остро.

Под этим понятием понимается защита информационной системы от случайных или преднамеренных вмешательств, наносящих вред владельцам или пользователям информации.

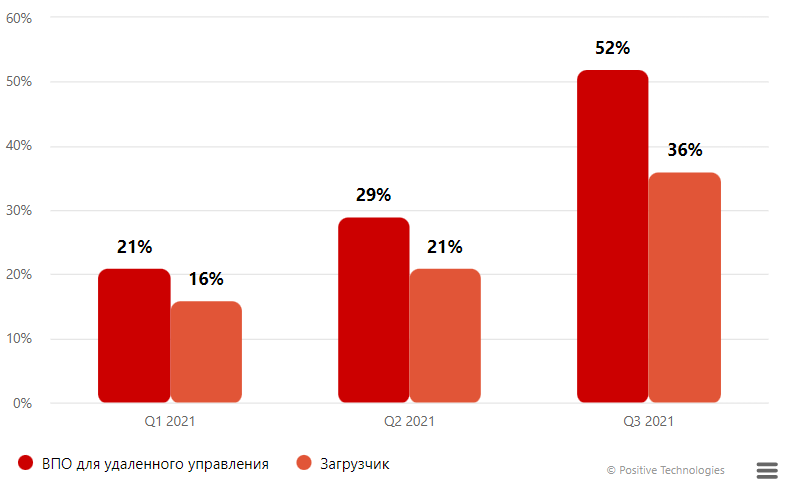
Обычно, в информационной безопасности выделяются три ключевых аспекта, нарушения в которых могут быть результатами вредоносного воздействия:

* Доступность: возможность получить запрашиваемую информационную услугу в разумные сроки;
* Целостность: актуальность и непротиворечивость информации, ее защита от уничтожения и несанкционированных изменений;
* Конфиденциальность: защита от несанкционированного чтения.

В данном реферате я постараюсь рассмотреть и проанализировать основные угрозы информационной безопасности, тренды, а также попытаюсь отследить их взаимосвязь с внедрением новых технологий.

# Атаки на отдельных лиц

При просмотре квартальной статистики за 2021 год одной из первых вещей, бросившихся в глаза, был рост использования вредоносного ПО для удаленного управления и загрузочных вирусов в атаках на частных лиц более чем в два раза(2):

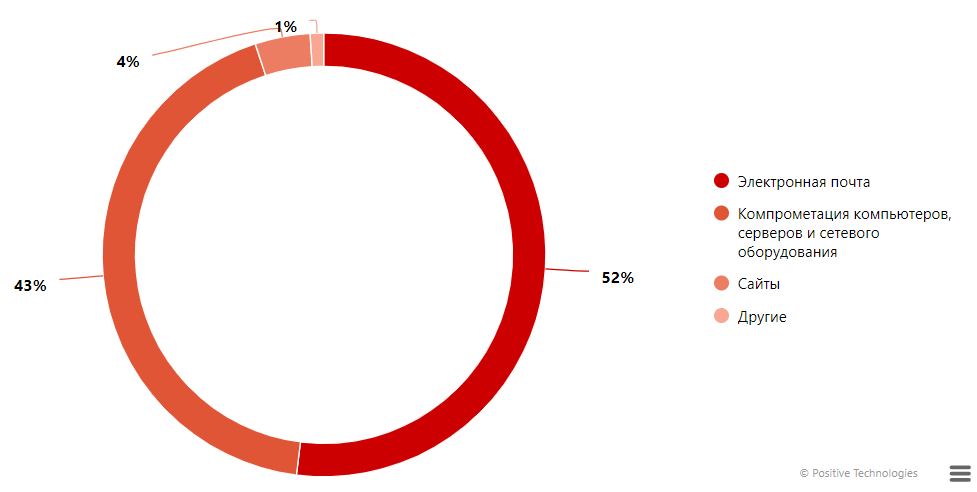


Новые загрузочные вирусы также отличаются разнообразием. Следует отметить разнообразие подходов злоумышленников к заражению жертв. Наблюдаются как и «классические» схемы (вирус встраивается в нелицензионную программу, загружаемую пользователям), так и заражение с использованием принципиально новых руткитов и уязвимостей. (1)(2)

В 62% случаев атаки злоумышленников на частных лиц приводили к утечке конфиденциальной информации; в основном похищались учетные данные (41% от общего объема украденных данных) и персональные (21%). Среди целей преступников всё чаще встречается майнинг криптовалюты на атакованных компьютерах. (2)

# Атаки на организации

Тем не менее, исходя из отчётов securelist.ru и positive technologies за последний квартал 2021 года (1)(2) большинство атак пришлось именно на организации. В этом нет ничего удивительного, поскольку как правило организации имеют большие бюджеты, чем частные лица; корпоративные тайны также могут представлять интерес для злоумышленников. Отчёты за предыдущие кварталы и годы подтверждают данную информацию. (3)(4)



На рисунке выше можно видеть статистику за 3 квартал 2021 года, описывающий способы распространения вредоносного ПО, ставящего своей целью именно организации.

В основном для атак на организации использовалась электронная почта, служащая средством доставки вредоносного ПО. Последней нашумевшей уязвимостью, распространявшейся по почте, можно назвать CVE-2021-40444, которая была отмечена сразу в нескольких источниках(1)(2).

В сентябре 2021 года компания Microsoft сообщила об уязвимости нулевого дня, которая позволяет злоумышленникам удаленно выполнять код на компьютерах. Уязвимость обнаружилась в браузерном движке Internet Explorer. И хотя сам браузер не очень популярен среди пользователей, некоторые программы (в частности, приложения Microsoft Office) используют его движок для обработки веб-контента. При открытии документа Microsoft Office скачивает вредоносный скрипт ActiveX по встроенной ссылке и запускает его. (1)(2) К концу месяца данная уязвимость была исправлена. (5) Жертвами данной уязвимости становились в первую очередь граждане Российской Федерации. (1)

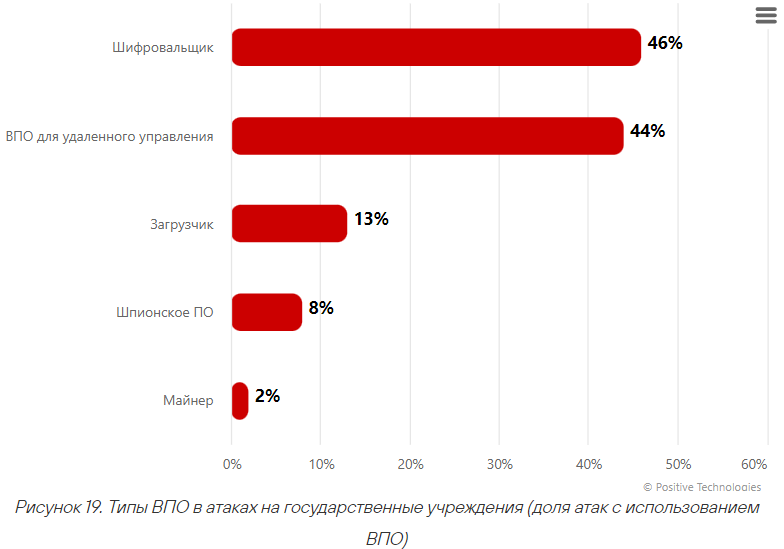
В целом, за последний год доля атак с использованием электронной почты уменьшилась с 62% до 52%. (3)(2) Можно предположить, что подобная динамика вызвана, отчасти, новой волной ограничений, направленной против пандемии COVID-19.

На втором месте находится компрометация сетевого оборудования, серверов и компьютеров. Именно подобную ситуацию можно связать с продолжающейся «удалёнкой». Сложно обеспечить должный уровень защиты информации в подобных условиях. Необходимость подключения к корпоративным сетям извне благоприятствует злоумышленникам, поскольку создаёт дополнительные возможности похитить данные организации.

Так, при атаках на государственные учреждения основном злоумышленники полагались на использование вредоносного ПО (45%) и социальной инженерии (42%).(2)

«Популярность» социальной инженерии как инструмента объяснима, поскольку удалённые сотрудники вынуждены во многом полагаться на собственные силы и знания при возникновении проблем, и иногда не имеют возможности своевременно получить помощь профильного специалиста по информационной безопасности. Значимость человеческого фактора остаётся высокой в условиях пандемии.

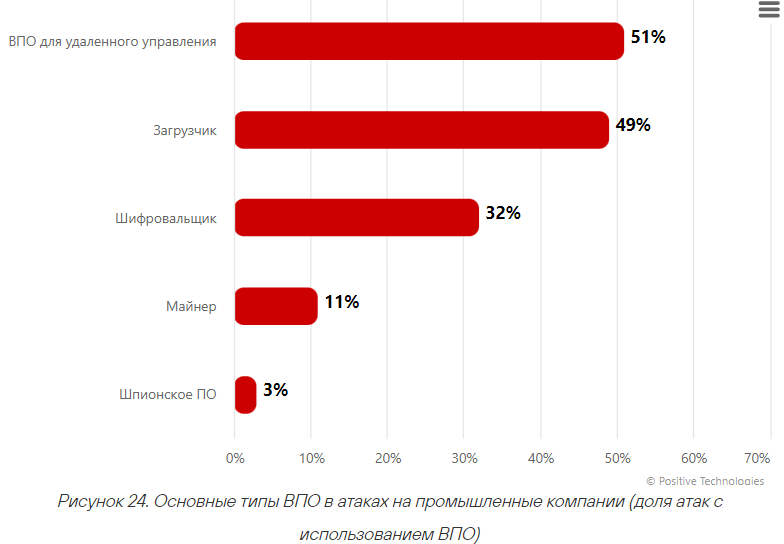
Ниже приведена статистика использования вредоносного ПО при атаке на госучреждения:



Как можно видеть, вредоносное ПО для удалённого управления часто используется и для атак на частных лиц, и для атак на организации (причём не только государственных (2)). Это можно объяснить «универсальностью» данного ПО (после успешного заражения, теоретически, поражённый узел можно использовать достаточно гибко) и благоприятными условиями именно для перехвата удалённого управления в связи с новым витком пандемии.

Следует сказать, что государственные учреждения занимают лидирующую позицию по количеству атак среди организаций, хотя по сравнению со II кварталом 2022 доля атак на них снизилась с 20% до 18%.

Статистика атак на промышленный сектор отличается от виденной ранее:



Динамика изменений за предыдущие месяцы (3)(4) свидетельствует об уменьшении доли шифрующего ПО, что может быть связано и с чрезмерным количеством внимания, которые привлекли к себе операторы шифровальщиков в прошлом квартале со стороны правоохранительных структур и исследователей безопасности. (2)

Лишний раз хочется отметить рост почти на 40% ПО, захватывающее удалённое управление. (3) Возможные причины были описаны выше.

Кроме этого, наличие доли майнеров в статистике выше подчёркивает, что набирающая популярность криптовалюта всё-таки влияет на «климат» информационной безопасности. Высокопроизводительное промышленное оборудование является «лакомым куском» для тех преступников, которые желают обогатиться за счёт чужих вычислительных мощностей.

# Криптовалюты

Криптовалюта – это цифровая платежная система, при проверке транзакций в которой не участвуют банки. Она хранится в цифровых кошельках, а криптовалютные платежи существуют исключительно в цифровом виде в онлайн-базе данных, описывающей конкретные транзакции. Несмотря на то, что операции с физическими деньгами не подразумеваются, возможен обмен с другой, «физической» валютой. (7)

Единицы криптовалюты (монеты) создаются в процессе майнинга. Этот процесс, при котором вычислительная мощность компьютера используется для решения сложных математических задач, в результате чего и генерируются монеты. (7)

Как можно было видеть в предыдущих разделах, подобным майнингом также можно заниматься нелегально, используя чужое оборудование без ведома его владельца.

Кроме этого, технология блокчейн, лежащая в основе криптовалют, освоена не до конца, поэтому существуют риски, что подобная искусственная финансовая система может быть взломана злоумышленниками. (7)

Так или иначе, на первом месте по количеству успешных нарушений остаётся социальная инженерия: пользователи «ведутся» на финансовые пирамиды и на прочие мошенничества. (7)

# Интернет вещей

Интернет вещей - сеть электронных устройств, оснащенных встроенными технологиями для взаимодействия друг с другом и внешней средой. Эта концепция стала неотъемлемой частью повседневной жизни, однако, в упомянутых выше источниках она практически не упоминается.

Тем не менее, хотя устройства Интернета вещей могут казаться безвредными, они не лишены проблем с безопасностью и конфиденциальностью, поскольку в их современной структуре существует множество угроз и уязвимостей. (7)

Современные устройства Интернета вещей могут быть заражены различными вредоносными программами на разных этапах своей работы. В большинстве случаев вредоносное ПО (вирусы, трояны и черви) обычно нацелено на локальную эксплуатацию и эксплуатацию на уровне операционной системы в зависимости от сложности атаки и её выполнения. Основная задача вредоносного ПО заключается в том, чтобы нарушить текущие операции и перехватить контроль над устройством. (7) Эти цели могут включать в себя, например:

* Доступ к личной информации, хранящейся на устройстве.
* Программная вставка сбоев в аппаратное обеспечение во время работы устройства.

Обычно, разработчики комбинируют аппаратные и программные средства для противодействия подобным угрозам (7):

* Устанавливают системы криптографической устойчивости и проводят микроархитектурный мониторинг событий.
* Использование аппаратных средств для обеспечения безопасной схемы управления ключами шифрования и обработки данных на оборудовании.

Многие из существующих устройств Интернета вещей имеют в своей основе много программных элементов (например, ОС), схожих с более привычными ЭВМ, и потому имеют общие уязвимости с ними. (7)

# Выводы

В данной работе были приведены основные понятия информационной безопасности. Была рассмотрена динамика 2022 года в области информационной безопасности. Одним из самых влиятельным факторов остаётся «удалёнка», открывающая уязвимости для злоумышленников. Одним из самых «популярных» видов вредоносного ПО является программа, перехватывающая удалённый контроль над компьютером. При этом люди всё так же остаются подверженными методам социальной инженерии.

Из упомянутых в начале реферата элементов «четвертой промышленной революции» в глобальной статистике по информационной безопасности упоминается, в первую очередь, криптовалюта и сопутствующий ей майнинг.

Тем не менее, это является следствием того, что нововведения не образуют принципиально новых сфер деятельности, а дополняют существующие. Поэтому, во многом, те меры защиты информации, которые существовали до внедрения этих элементов, остаются актуальны и на данный момент.

# Список использованных источников

1. Развитие информационных угроз в третьем квартале 2021 года. - Текст: электронный, SecureList.ru, 26.11.2021. – URL: <https://securelist.ru/it-threat-evolution-q3-2021/103948/> (дата обращения: 28.02.2022).
2. Актуальные киберугрозы: III квартал 2021 года. - Текст: электронный, Positive Technologies, 08.12.2021. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/> (дата обращения: 28.02.2022).
3. Актуальные киберугрозы: I квартал 2021 года. - Текст: электронный, Positive Technologies, 11.06.2021. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/> (дата обращения: 28.02.2022).
4. Актуальные киберугрозы: II квартал 2021 года. - Текст: электронный, Positive Technologies, 30.08.2021. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/> (дата обращения: 28.02.2022).
5. How To Fix The CVE-2021-40444 A New 0-Day MSHTML Remote Code Execution Vulnerability Targeting Windows Users? - Текст: электронный, The SecMaster, 16.09.2021. – URL: <https://www.thesecmaster.com/how-to-fix-the-cve-2021-40444/#:~:text=Microsoft%20has%20released%20the%20fix,ActiveX%20controls%20in%20Internet%20Explorer> (дата обращения: 28.02.2022).
6. Информационная безопасность устройств IoT c использованием аппаратной поддержки. – Текст: электронный. Хабр, 21.12.2020. – URL: <https://habr.com/ru/post/534300/> (дата обращения: 28.02.2022).
7. Что такое криптовалюта и как она применяется? – Текст: электронный. Лаборатория Касперского, 2021. – URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-cryptocurrency> (дата обращения: 28.02.2022).