Карпухин Алексей Денисович,
курсант 223 учебной группы, 2 факультета,
Филиал ВУНЦ ВВС ВВА в г. Челябинск

Цыганко Александр Валерьевич,
Старший преподаватель,
Филиал ВУНЦ ВВС ВВА в г. Челябинск

СОВРЕМЕННЫЕ ВЫЗОВЫ В ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ: КИБЕРУГРОЗЫ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Аннотация: В статье рассматриваются современные вызовы, стоящие перед службами защиты государственной тайны в условиях развития киберугроз. Описаны основные методы атак, способы противодействия, а также роль сотрудников в обеспечении информационной безопасности. Приведён реальный пример успешной кибератаки на государственные структуры, подчёркивающий необходимость постоянного совершенствования системы защиты.

Ключевые слова: государственная тайна, киберугрозы, информационная безопасность, фишинг, SolarWinds, защита информации.

В условиях стремительного развития цифровых технологий значение государственной тайны значительно возросло. Информация, представляющая государственную или военную ценность, стала одной из главных целей для киберпреступников, иностранных разведок и иных недружественных сил. Защита государственной тайны в XXI веке требует не только традиционных мер безопасности, но и эффективных методов противодействия новым угрозам в киберпространстве [3] [4].

Новые вызовы в сфере защиты государственной тайны

С каждым годом увеличивается количество и сложность кибератак на государственные учреждения. Злоумышленники используют широкий спектр методов: от традиционных хакерских атак до социальных инженерий, нацеленных на обман сотрудников для получения доступа к конфиденциальной информации. Угроза также исходит от инсайдеров – лиц, имеющих легальный доступ к тайным данным и нарушающих режим их охраны. Особое внимание привлекает активность иностранных разведывательных служб, системно работающих над получением секретной информации с применением передовых технологий [3].

Киберугрозы как главный фактор риска

Киберугрозы стали одним из ключевых факторов риска для государственной тайны. Основные методы атак включают:

- Фишинг – рассылка электронных писем с вредоносными вложениями или ссылками для кражи учётных данных.
- Эксплойты уязвимостей – использование слабых мест в программном обеспечении для несанкционированного проникновения.
- Вредоносное ПО – программы-шпионы, трояны и вирусы, обеспечивающие удалённый доступ к защищённым системам.

Реальный пример:

В 2020 году произошла крупная кибератака на ряд правительственных агентств США, известная как операция SolarWinds. Злоумышленники внедрили вредоносный код в обновления

программного обеспечения компании SolarWinds, которое использовалось для управления IT-инфраструктурой множества государственных органов. В результате хакеры получили доступ к закрытым сетям и имели возможность перехватывать конфиденциальную информацию в течение нескольких месяцев до обнаружения атаки. Этот случай показал, насколько уязвимыми могут быть даже высокозащищённые системы через цепочки поставок [3] [4] [1] [2].

Меры информационной безопасности

Для противодействия современным киберугрозам необходимо внедрение комплексных мер безопасности, включая:

- Шифрование данных
- Многоуровневая аутентификация
- Системы мониторинга и реагирования
- Политика ограниченного доступа

Эффективная защита возможна только при регулярном обновлении технических средств и политик безопасности [3] [4].

Роль сотрудников и подготовка кадров

Человеческий фактор остаётся одной из основных уязвимостей в защите государственной тайны. Поэтому важнейшее значение приобретает:

- Обучение персонала
- Проверка благонадёжности
- Культура безопасности

Нарушение режима секретности, даже непреднамеренное, может повлечь за собой серьёзные последствия, включая уголовную ответственность [4].

Киберугрозы представляют собой одну из самых серьёзных проблем в сфере защиты государственной тайны в современном мире. Для эффективной защиты требуется комплексный подход, включающий:

1. Постоянное совершенствование технологий защиты
2. Развитие компетенций персонала
3. Создание систем оперативного мониторинга и реагирования
4. Внедрение политики нулевого доверия
5. Повышение устойчивости к атакам через цепочки поставок [3] [4]

Только при соблюдении всех перечисленных мер возможно надёжное обеспечение государственной тайны в условиях стремительно меняющегося цифрового мира.

Список литературы:

1. CISA. (2020). Улучшение защиты от кибератак.. https://www.cisa.gov/news-events/alerts/2020/12/17/cisa-updates-guidance-solarwinds-cyberattack
2. Microsoft. (2020). Cyberattacks and SolarWinds: What you need to know. https://blogs.microsoft.com/on-the-issues/2020/12/13/cyberattacks-solarwinds-fireeye/
3. Российский институт стратегических исследований (РИСИ). Современные угрозы информационной безопасности. http://riss.ru/article/9399/
4. Президент Российской Федерации. Доктрина информационной безопасности Российской Федерации. http://www.kremlin.ru/acts/bank/41460