УДК 004.056

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Голубев С.В., кандидат экономических наук, доцент,
тел. 8(8422) 55-91-12, des-s@mail.ru
Голубева С.А., кандидат экономических наук, доцент,
тел. 8(8422) 55-91-12, golubevas83@mail.ru
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *информационная безопасность, интернет вещей, киберугрозы, облачные технологии, цифровизация.*

Статья посвящена актуальным вопросам информационной безопасности: атаки на цепочки поставок и на третьих лиц, атаки на элементы «интернета вещей» и вопросы защиты облачных технологий, безопасность персональных данных, применение искусственного интеллекта в информационной безопасности.

Введение. Скорость развития и изменения информационного пространства в последнее время поражает не только обычных пользователей, но и специалистов в области информационной безопасности. Происходит бурное развитие как объема обрабатываемой информации и количества подключенных к интернету устройств, так и самих подходов и систем, а также тотальная цифровизация и переход в онлайн многих сервисов. Последние события в мировой экономике еще больше ускорили этот тренд. Широкое использование высокоуровневых языков программирования, развитие облачных инфраструктур и технологий виртуализации позволяет разработать новое приложение в кратчайшие сроки. Вместе с этим развиваются и киберберугрозы, поскольку злоумышленники используют те же инструменты разработки, но в своих целях. Это выводит уровень информационной безопасности на новый уровень. Если раньше борьба со злоумышленниками сводилась к противостоянию профессионалов и средств защиты информации, то теперь это превратилось в полноценную кибервойну, в которой участвуют искусственные интеллекты [1].

Результаты исследований и их обсуждение. Существует несколько вопросов информационной безопасности, актуальных в настоящее время:

1. Атаки на цепочки поставок.
2. Атаки на третьих лиц.
3. Атаки на элементы «интернета вещей».

4. Облачные технологии.

5. Безопасность персональных данных.

6. Применение искусственного интеллекта в информационной безопасности.

1. Крупные компании в настоящее время серьезно подходят к вопросам информационной безопасности и включают в работу такие процессы, как управление сетевыми рисками, уязвимостями и обновлениями, средства защиты информации, сбор и анализ логов. Но современное программное обеспечение стало настолько сложно, что даже высококвалифицированный специалист может многое не знать и приходится полагаться на поставщиков операционных систем, прикладного программного обеспечвения и даже самих средств защиты. Поэтому многие организации становятся зависимыми от знаний и компетенций самого поставщика.

Защита от атак на цепочки поставок заключается в разработке мероприятий, направленных на проверку надежности вендора и состояние информационной безопасности конкретного поставщика. Для этого применимы классические инструменты экономической безопасности, например, запрос информации в «Интерфакс-СПАРК» и «Контур-Фокус», а также встреча с руководством. Также можно использовать анализ поведения установленных программ и их сетевую активность [2].

2. Атаки на третьих лиц. Их отличие заключается в том, что атакованные контрагенты могут, сами того зная, стать опорным пунктом для атакующего. Для этого используются существующие между контрагентами удаленное подключение через VPN-туннель и использование ранее созданной учетной записи для разработчика. Хакеры могут сначала атаковать подрядчика, и если он защищен хуже, то через него добраться до первоначальной цели [3].

Такую атаку легко предотвратить. Для этого возможно применить принцип «нулевого доверия», т.е. проверка и контроль всех учетных записей и устройств вне зависимости от того, кто является их инициатором.

3. Определение «Интернет вещей» (IoT - internet of things) подразумевает большое количество элементов электроники потребительского уровня, непрерывно подключенных к разнообразным сетями, в т.ч. к интернет, для взаимодействия между собой, с владельцем и с разнообразными интернет-сервисами. Примерами IoT-устройств могут быть: смарт-телевизоры, «умные колонки», фитнес-трекеры и т.д. [4].

Особую опасность вызывают IoT-устройства, допускающие внешнее подключение к ним, но программы которых не получают обновлений безопасности от производителя. Поиск уязвимостей в таких устройствах

затруднителен, в том числе за счет установки на них самого простого софта с урезанным функционалом.

В случае применения устройств «интернета вещей» для выполнения бизнес-задач, рекомендуется внимательно отнестись к выбору производителя, отдавая предпочтение тому, кто регулярно выпускает обновления встроенного ПО. Предоставляет продолжительную гарантию и рекомендации по защищенной настройке устройства.

В случае применения IoT-устройств в личных целях следует оценить, насколько тот или иной функционал удаленной работы с устройством действительно требуется, насколько простой будет защищенная настройка устройства конечным пользователем.

4. Защита облачных инфраструктур в настоящее время является крайне важной задачей, что безусловно связано с популярностью облачных технологий. Их можно разделить на следующие типы:

- Public cloud (публичные облака) - провайдер облачных услуг предоставляет заказчику свою инфраструктуру и сервисы на коммерческой основе, как правило, по подписке.
- Private cloud (частные облака) - организация размещает часть своей инфраструктуры в некотором своем или арендуемом ЦОД (центре обработки данных) и полностью контролирует все аппаратные и программные компоненты.
- Hybrid cloud (гибридные облака) - организация совмещает работу с публичным и частным облаком, размещая свои приложения и данные в зависимости от удобства и потребностей в той или иной инфраструктуре.
- Multi-cloud (мультиоблако) - организация пользуется услугами нескольких провайдеров облачных сервисов для надежности и повышения отказоустойчивости, например, размещая основную инфраструктуру в одном публичном облаке, а бекапы и резервные сервисы - в другом [5].

5. Вопросы обеспечения конфиденциальности персональных данных стали подниматься практически сразу после начала широкого применения средств вычислительной техники для обработки информации, касающейся физических лиц. Еще в 1981 году была подписана Конвенция №108 Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Высокая социальная значимость обеспечения информационной безопасности персональных данных была и остается главной движущей силой государственных законодательных актов. Например, Федеральный Закон №152 «О персональных данных» от 27.07.2006 г. При этом

законодательные нормы непрерывно актуализируются для соответствия изменяющемся киберугрозам.

С точки зрения бизнеса, защита персональных данных клиентов и сотрудников является важной задачей не только в контексте соответствия законодательству - сегодня зачастую именно накопленные данные о потребителях представляют собой один из главных нематериальных активов компании, а лояльность сотрудников и клиентов формируется в том числе и мерами, предпринимаемыми компанией для защиты их аккаунтов, личных данных, платежной информации.

Еще более важной задачей является защита биометрических персональных данных - биологических, физиологических, поведенческих характеристик человека, используемых для установления личности (идентификации, аутентификации). Биометрия уже широко используется финансовыми организациями для дистанционного получения банковских услуг в рамках российской «Единой биометрической системы», которая также позволяет выполнять ряд других юридически значимых действий удаленно, а также в транспортной сфере для обеспечения безопасности, в проектах распознавания пассажиров в аэропортах и бесконтактной оплаты проезда в метрополитене. Коммерческие компании зачастую используют биометрические персональные данные клиентов для подтверждения личности, а также для контроля доступа своих сотрудников в помещения [6].

Для защиты персональных данных в современной ИТ-инфраструктуре можно руководствоваться следующими принципами на всех этапах обработки информации:

- Безопасность при хранении данных.
- Безопасность при передаче данных.
- Безопасность при обработке данных.
- Конфиденциальность по умолчанию.
- Встроенная конфиденциальность.

6. Разговоры о практическом применении искусственного интеллекта, в том числе и в информационной безопасности, ведутся уже давно, но на рынок данные инструменты вышли тогда, когда точность работы стала оправдывать их стоимость, а возможности злоумышленников стали широки настолько, что эффективно и оперативно противостоять им стало возможно только с применением данной технологии.

Использование искусственного интеллекта в информационной безопасности обосновано прежде всего двумя факторами - необходимостью оперативного реагирования при наступлении инцидента и нехваткой квалифицированных специалистов по киберзащите. Системы защиты на основе

искусственного интеллекта будут незаменимы для выявления аномалий в большом количестве событий информационной безопасности, например, путем анализа журналов СЗИ, данных из SIEM-систем или SOAR-решений. Детектирование аномалий может помочь в защите пользовательских данных. Финансовые организации могут использовать системы машинного обучения и искусственного интеллекта также для проведения оценки (скоринга) заемщиков, анализа финансовых рисков, в анти-фрод системах. Другой моделью использования систем искусственного интеллекта в кибербезопасности является работа с внутренними нарушителями: зная типичное поведение пользователя, система может отправить предупреждение аналитикам в случае существенного изменения модели работы. Системы защиты, оснащенные компьютерным зрением и обработкой речи, смогут оперативно оповещать охрану о попытках прохода через проходную посторонних или сотрудников по чужим пропускам, анализировать рабочую активность сотрудников с помощью веб-камер, оценивать корректность общения менеджеров с клиентами по телефону.

При этом не следует забывать и то, что системы на базе искусственного интеллекта используют и киберпреступники: известны мошеннические приемы использования Deep fake (создание реалистичного виртуального образа человека) для обмана анти-фрод систем, подделки голосов для мошеннических звонков родственникам атакованных лиц с просьбой перевести деньги, применения телефонных IVR-технологий для фишинга и хищения денежных средств. Во вредоносном ПО также используются элементы искусственного интеллекта, которые позволяют атакующим гораздо быстрее повышать свои привилегии, перемещаться по корпоративной сети, а затем находить и похищать интересующие их данные.

Заключение. Таким образом, технологии, ставшие доступными широкой публике, используются как во благо, так и во вред, что означает, что бороться с такими подготовленными киберпреступниками можно и нужно с применением самых совершенных средств и методов защиты.

Библиографический список

1. Голубев, С.В. Экономическая эффективность внедрения информационных технологии в производство / С.В. Голубев, С.А. Голубева, В.А. Голубев // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения. Том 1. – Ульяновск: УлГАУ, 2019. – с. 255-257.

2. Миначева Э.Ф. Фишинг как метод социальной инженерии в финансовом мошенничестве / Э.Ф. Миначева, С.В. Голубев //

Материалы IV Международной студенческой научной конференции: В мире научных открытий. Ульяновск: УлГАУ, 2020. – с. 112-115.

3. Бураева, Л.А. Актуальные проблемы защиты информации в коммуникационных системах на современном этапе / Л.А. Бураева, Т.М. Шогенов // Научные исследования: теория, методика и практика : материалы II Междунар. науч.-практ. конф. (Чебоксары, 27 авг. 2017 г.) / редкол.: О.Н. Широков [и др.] – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 211-213.

4. Шогенов, Т.М. О некоторых вопросах противодействия экстремизму в сети Интернет // Пробелы в российском законодательстве. – 2017. – №3. – с. 58–59.

5. Машкина, И.В. Обеспечение информационной безопасности системы облачных вычислений / Машкина И.В., Сенцова А.Ю. // Информационные технологии. - 2016. - Т. 22. - № 11. - с. 843-853

6. Малюк, А.А. Зарубежный опыт формирования в обществе культуры информационной безопасности / А.А. Малюк, О.Ю. Полянская // Безопасность информационных технологий. - 2016. - № 4. - с. 25-37.

CURRENT ISSUES OF INFORMATION SECURITY

Golubev S.V., Golubeva S.A.

***Key words**: information security, internet of things, cyber threats, cloud technologies, digitalization.*

The article is devoted to topical issues of information security: attacks on supply chains and third parties, attacks on elements of the "Internet of Things" and issues of protecting cloud technologies, personal data security, the use of artificial intelligence in information security.