УДК 004.9

Кузьмичева Т.Г., кандидат физико-математических наук, доцент
доцент кафедры «Прикладной информатики и информационных технологий»,
Белгородский государственный национальный исследовательский университет
Россия, г. Белгород
Голованова Е.В., кандидат физико-математических наук, доцент
доцент кафедры «Прикладной информатики и математики»,
Белгородский государственный аграрный университет им. В.Я. Горина
Россия, п. Майский, Белгородский район, Белгородская область

СФЕРЫ ПРИМЕНЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Аннотация: кибербезопасность – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес - сферы до мобильных технологий.
Ключевые слова: кибербезопасность, мобильные технологии, интерактивные технологии, операционная безопасность, безопасность сетей, безопасность приложений.

Kuzmicheva T. G., candidate of physical and mathematical Sciences, associate Professor associate Professor of "Applied Informatics and information technologies», Belgorod state national research University Russia, Belgorod
Golovanova E.V., Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of «Applied Informatics and Mathematics», Belgorod State Agrarian University named after V.Ya. Gorin
Russia, Maysky village, Belgorod district, Belgorod region

CYBERSECURITY APPLICATIONS

Abstract: cybersecurity is a set of methods and practices for protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Cybersecurity has applications in a wide variety of fields, from business to mobile technology.
Keywords: cybersecurity, mobile technologies, interactive technologies, operational security, network security, application security.

Кибербезопасность находит применение в самых разных областях, от бизнес - сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

Безопасность сетей – действия по защите компьютерных сетей от различных угроз, например целевых атак или вредоносных программ.

Безопасность приложений – защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.

Безопасность информации – обеспечение целостности и приватности данных, как во время хранения, так и при передаче [1].

Операционная безопасность – обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.

Аварийное восстановление и непрерывность бизнеса – реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как организация будет бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай,

если организация теряет доступ к определенным ресурсам из-за атаки злоумышленников.

Повышение осведомленности – обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства.

Чаще всего утечке данных подвергаются медицинские и государственные учреждения или организации из сферы розничной торговли. В большинстве случаев причина – действия преступников. Некоторые организации привлекают злоумышленников по понятной причине – у них можно украсть финансовые и медицинские данные. Однако мишенью может стать любая компания, ведь преступники могут охотиться за данными клиентов, шпионить или готовить атаку на одного из клиентов.

Очевидно, что масштаб киберугроз будет расширяться, следовательно, глобальные расходы на решения по кибербезопасности будут увеличиваться. По прогнозам Gartner, в целом расходы на кибербезопасность в мире достигнут $188,3 млрд. в 2023 году, а к 2026 году превысят $260 млрд. Правительства разных стран борются с преступниками, помогая организациям внедрять эффективные методы кибербезопасности.

Так, Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) разработал принципы безопасной IT-инфраструктуры. NIST рекомендуют проводить постоянный мониторинг всех электронных ресурсов в реальном времени, чтобы

выявить вредоносный код, пока он не нанес вреда, и предотвратить его распространение.

Национальный центр кибербезопасности (National Cyber Security Centre) правительства Великобритании выпустил руководство 10 steps to cyber security (10 шагов к кибербезопасности). В нем говорится о том, насколько важно вести наблюдение за работой систем. В Австралии рекомендации по борьбе с новейшими киберугрозами регулярно публикует Австралийский центр кибербезопасности (Australian Cyber Security Centre, ACSC).

По мере того как мир становится все более взаимосвязанным и зависимым от технологий, а мы все чаще ведем свой бизнес и жизнь в интернете, мы создаем все больше возможностей для киберпреступников, методы которых становятся все более изощренными.

Кибербезопасность борется с тремя видами угроз.

Киберпреступление – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.

Кибератака – действия, нацеленные на сбор информации, в основном политического характера.

Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Как злоумышленникам удается получить контроль над компьютерными системами? Они используют различные инструменты и приемы.

Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники

используют его, чтобы заработать или провести атаку по политическим мотивам [2].

Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:

Вирусы – программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.

Троянцы – вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.

Шпионское ПО – программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.

Программы-вымогатели шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.

Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.

Использованные источники:

1. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012.
2. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.