§ 15. Кибербезопасность и киберустойчивость

15.1. Кибербезопасность

Термин «кибербезопасность» объединяет в себе слова «кибер» и «безопасность». Начнем с безопасности.

Безопасность — это состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз.

Угроза безопасности — это возможность воздействия на систему или объект, которое может нарушить безопасность.

В зависимости от сфер интересов различают несколько видов безопасности. В сфере экономики — экономическая безопасность, в сфере экологии — экологическая безопасность и т. д.

Ключевое значение в современном мире приобрела информационная сфера, которая оказывает всеобъемлющее влияние на проходящие экономические, политические и социальные процессы.

Информационная безопасность — это состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Понятие информационной безопасности введено у нас в стране на законодательном уровне (пример 15.1).

Основными объектами информационной сферы являются *информационные системы*, которые включают банки данных, информационные технологии и комплекс программно-технических средств (пример 15.2).

Пример 15.1. Термин «информационная безопасность» введен в Концепции информационной безопасности Республики Беларусь, утвержденной Советом Безопасности Республики Беларусь в 2019 году.

В Концепции целью обеспечения информационной безопасности поставлено достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

Внимание к информационной безопасности на государственном уровне вызвано тем, что объекты промышленности, транспорта, энергетики, электросвязи, здравоохранения построены на базе компьютерных систем. Это ставит жизнь и здоровье населения в прямую зависимость от надежности этих компьютерных систем и защищенности информации в них.

Пример 15.2. Термин «информационная система» введен в Законе Республики Беларусь «Об информации, информатизации и защите информации», принятом в 2008 году.

Информационные системы предназначены для хранения, обработки, поиска, распространения, передачи и представления информации. По степени распределенности они делятся на локальные (настольные) и распределенные.

Примеры локальных информационных систем — это пакеты офисных программ (MS Office, OpenOffice и др.), системы программирования, системы управления базами данных (СУБД).

В распределенных информационных системах компоненты распределены по нескольким компьютерам. Примерами могут быть информационные системы предприятий, учреждений и организаций, автоматизированные системы управления производственными процессами, базы данных и информационно-поисковые системы в Интернете.

Пример 15.3. Слово «кибер» возникло в английском языке как часть слова «кибернетика», которое является названием науки об общих законах управления, связи и переработки информации.

Слово «кибер» вначале обозначало слово «кибернетический» и впервые стало использоваться писателями-фантастами. Именно в фантастике возникло слово «киберпространство».

В русскоязычной фантастике киберами называли разновидность роботов.

Пример 15.4. Киберпространство — понятие для обозначения виртуальной реальности.

Киберспорт (компьютерный спорт) — командные или индивидуальные соревнования по компьютерным видеоиграм, которые имитируют реальные спортивные состязания.

Кибербуллинг — это анонимные намеренные оскорбления, угрозы, нападки на человека при помощи Интернета.

Кибертерроризм — это воздействия на информационные системы, несущие угрозу здоровью и жизни людей, применяемые для устрашения населения либо для дестабилизации общественного порядка.

Пример 15.5. *Целостность информации* означает, что изменение информации может быть только контролируемым.

Конфиденциальность информации означает, что лицо, получившее к ней доступ, не имеет права передавать ее другим лицам.

Подлинность информации означает, что точно установлено авторство информации.

Доступность информации означает, что лицо, имеющее доступ к информации, реализует этот доступ беспрепятственно.

Сохранность информации означает, что при любых обстоятельствах информация не будет безвозвратно потеряна.

Технические средства, системы и технологии хранения, передачи и обработки информации образуют *информационную инфраструктуру* предприятия, организации или государства.

Кибербезопасность — это состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Таким образом, кибербезопасность — это раздел информационной безопасности.

«Кибер» — приставка, которая означает «связанный с компьютерами и Интернетом» и имеет интересную историю (пример 15.3). Известно немало терминов, которые используют это слово-приставку (пример 15.4).

Кибербезопасность предполагает защищенность информации в информационной инфраструктуре. В соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации» защита информации должна обеспечивать *целостность*, *конфиденциальность*, *подлинность*, *доступность* и *сохранность* информации. В примере 15.5 приведены описания этих ее свойств.

Защита информации — это не простая задача, так как количество данных со временем растет лавинообразно. Только с 2010 по 2020 год объем хранимой во всем мире информации вырос в 50 раз. Число серверов американских компаний Google и Amazon исчисляется миллионами.

15.2. Уязвимость информационной инфраструктуры

Кибербезопасность предполагает защищенность информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Угрозы возникают, если информационная инфраструктура имеет уязвимость.

Уязвимость — свойство информационной инфраструктуры или ее объектов, которое позволяет реализовать угрозу (воздействовать на инфраструктуру).

Воздействие на информационную инфраструктуру или ее объекты может быть *случайным* или *умышленным* (пример 15.6).

Умышленное воздействие на информационную инфраструктуру программными или программно-техническими средствами называется ***кибератакой***.

Основная цель умышленных воздействий — получение финансовой выгоды. Для этого используют как вымогательство, так и хищение ценной информации (персональные данные аккаунтов, данные доступа к платежным сервисам).

Уязвимость могут иметь информационная инфраструктура в целом, ее технические и программные средства, персонал и пользователи.

Если антивирусные средства инфраструктуры имеют уязвимость, то вирусная кибератака может достигнуть успеха (пример 15.7).

Пример 15.6. Случайное воздействие может являться следствием ошибочных действий персонала, внезапных отказов технических средств и т. д.

Умышленные воздействия подразделяются на активные и пассивные.

Пассивные воздействия направлены на несанкционированное использование информационных ресурсов, например подслушивание, видеозапись.

Активными умышленными воздействиями являются внедрение вредоносных программ в компьютеры пользователей, мошенническое использование сайтов информационных услуг и др.

Простейший и распространенный способ умышленного воздействия — это фишинг (упоминался в пособии для 9-го класса). Представляет собой рассылку электронных писем или сообщений в соцсетях от имени коллег по работе, сотрудников банка или представителей государственного учреждения. Цель фишингового письма — заставить получателя немедленно перейти на поддельный веб-сайт, весьма похожий на известный, и там ввести конфиденциальную информацию, чтобы избежать якобы внезапно возникшую опасность или каких-то серьезных последствий бездействия. Умышленные воздействия, реализующие угрозы кибербезопасности, в соответствии с Уголовным кодексом Республики Беларусь могут быть квалифицированы как преступления против информационной безопасности.

Пример 15.7. Вирусы заражают файлы специфическим кодом. Троянцы — вредоносные программы, которые прячутся под маской легального программного средства. Шпионские программы тайно следят за действиями пользователя и собирают финансовую персональную информацию. Программы-вымогатели шифруют файлы и данные, а преступники требуют выкуп за восстановление.

Пример 15.8. Уязвимость программного средства может быть результатом ошибок программирования, но чаще это непредусмотренное свойство, которое разработчику выявить очень сложно. Проверкой работоспособности программ занимаются тестировщики, а поиском уязвимости — злоумышленники.

Пример 15.9. В приложениях пакета MS Office уязвимость находят постоянно, и разработчики постоянно создают и рассылают обновления, которые закрывают найденную уязвимость.

Это противостояние злоумышленников и разработчиков ведется уже давно.

С появлением новых информационных технологий и новых программных средств можно ожидать появления новых уязвимостей и новых угроз.

Пример 15.10. В августе 2013 г. были взломаны аккаунты с персональными данными более 3 млрд пользователей компании Yahoo!.

В 2018 г. оказались взломанными аккаунты более 500 млн клиентов гостиничной сети Marriott, 440 млн пользователей программного обеспечения Veeam, 300 млн клиентов логистической компании SF Express.

В августе 2020 года в Интернете появилась незащищенная база данных, содержащая персональные данные около 235 млн пользователей сервисов Instagram, TikTok и YouTube.

Пример 15.11. Успех распределенных сетевых атак основан на уязвимости серверов компьютерной сети, которые всегда имеют ограничения по количеству одновременно обрабатываемых запросов. Если число запросов превышает предельные возможности сервера, то результатом может быть полное прекращение его нормальной работы — отказ в обслуживании.

Большой проблемой являются уязвимость операционных систем и приложений (пример 15.8). Как только злоумышленники находят слабое место программы, они создают свой зловредный программный код, который называется «эксплойт», и, атакуя, пытаются внедрить его в программу (пример 15.9).

По оценкам экспертов, кибератакам эксплойтов-вымогателей компании во всем мире подвергаются каждые 14 с. Масштабы хищения персональных данных пользователей с серверов сети впечатляют еще больше (пример 15.10).

Другой вид кибератак — *распределенные сетевые атаки*. Их называют также атаками типа «отказ в обслуживании» (по-английски Distributed Denial of Service) или DDoS-атаками (пример 15.11).

Обычная цель DDoS-атаки — вымогательство денег за прекращение атаки, дискредитация бизнес-конкурента или нанесение ему ущерба.

С каждым годом число кибератак растет. При этом набор приемов, которые используют злоумышленники, пополняется почти ежемесячно.

Но самым уязвимым местом кибербезопасности был и будет человеческий фактор — поведение сотрудников и пользователей.

Согласно статистике 91 % атак на банки совершают коррумпированные сотрудники самих банков, 8 % — банковские посредники и только 1 % приходится на хакеров.

По результатам исследований, потери российского пользователя в ходе ки-

бератак составляют в среднем 80 долларов, а каждая девятая жертва теряет более 1000 долларов (пример 15.12).

Для получения конфиденциальной информации злоумышленники широко используют социальную инженерию. Это психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации (пример 15.13).

15.3. Обеспечение кибербезопасности. Киберустойчивость

Грамотный подход к кибербезопасности предполагает реализацию системы мер защиты информационной инфраструктуры.

Обеспечение кибербезопасности — это система мер противодействия угрозам информационной безопасности.

Следует заметить, что в Интернете понятие «обеспечение кибербезопасности» часто называют кибербезопасностью (в широком смысле).

Обеспечение кибербезопасности — это воплощение всех мер защиты сетей, устройств и приложений, защиты конфиденциальности и целостности данных, а также мер сохранения нормальной работы информационной инфраструктуры в целом (пример 15.14).

В системе мер обеспечения кибербезопасности особое место занимает обучение пользователей. Пользователь и его цифровое устройство — это популярная цель злоумышленников. Взломав индивидуальное цифровое

Пример 15.12. Причиной потери 21 % пострадавших назвали предоставление мошенникам доступа к записям в платежном сервисе, 19 % — ввод своих конфиденциальных данных на поддельном веб-сайте.

Пример 15.13. Мошенник вступает в контакт с пользователем, притворяясь сотрудником банка, продавцом или покупателем Интернет-сервиса, доверенным лицом сервиса и т. д. Цель — психологически вынудить пользователя сообщить свои персональные данные злоумышленнику или на сайт, который злоумышленник указывает.

Пример 15.14. Система мер противодействия угрозам информационной безопасности образует несколько уровней защиты как внутри инфраструктуры, так и на ее периметре. На каждом уровне реализуются определенные принципы и средства контроля.

Первую линию защиты сетей обеспечивают межсетевые экраны, которые осуществляют мониторинг входящего и исходящего сетевого трафика. Межсетевой экран может быть аппаратным, программным или смешанного типа.

Стратегия DLP (data-loss prevention), которую реализуют специалисты по информационной безопасности, позволяет контролировать возможные пути утечки данных.

Защиту информации обеспечивают системы идентификации по биометрическим данным, системы криптографической защиты каналов передачи и носителей данных, программные решения для управления ключами шифрования.

В последние годы шифрование данных стало нормой в работе с веб-сайтами.

Пример 15.15. В учебном пособии «Информатика» для 9-го класса был приведен ряд эффективных мер безопасности пользователя в сети Интернет. В дополнение к ним приведем следующие меры:

1. Регулярно выполняйте резервное копирование данных, которое дает гарантии сохранности уникальной информации. В случае кражи или шифрования такой информации вымогательство не пройдет. Восстановить информацию из резервных копий можно в любой момент.

2. Обновляйте операционную систему приложения. Используя обновления, вы получаете свежие исправления уязвимости.

3. Внимательно относитесь к тому, что подключаете к компьютеру. Вредоносные программы могут распространяться через зараженные флешки, внешние жесткие диски и даже смартфоны.

4. Избегайте незащищенных сетей Wi-Fi в общественных местах. Подключившись к незащищенной сети Wi-Fi, вы можете подвергнуться атаке Man-in-the-Middle («Человек посередине»). Это атака, в ходе которой злоумышленник перехватывает данные во время их передачи. Он как бы становится промежуточным звеном в информационной цепочке, а жертва об этом даже не подозревает и может передать ценную информацию.

5. Банковские операции или покупки выполняйте только на принадлежащем вам устройстве в сети, которой вы доверяете.

6. Следите за сохранностью своих цифровых устройств (смартфона, планшета и ноутбука). Не допускайте к их использованию незнакомцев.

7. Как правило, стереть данные из Интернета невозможно. Все, что попало в Интернет, останется там навсегда. Единственный способ избежать утечки информации — не делиться ею.

устройство, можно получить доступ не только к информации в нем, но и к конфиденциальной информации в сети.

Меры обеспечения кибербезопасности для пользователей часто формулируют как меры или правила безопасности пользователя (пример 15.15).

Эффективная система мер противодействия угрозам информационной безопасности переводит информационную инфраструктуру в новое состояние — в состояние киберустойчивости.

Киберустойчивость — способность информационной инфраструктуры успешно предотвращать реализацию угроз или быстро восстанавливаться после их реализации.

Кибератака на уровне пользователя может привести к самым разным последствиям.

Технические решения не смогут защитить от угроз, если злоумышленник-профессионал завладеет вашим доверием. Многие из них действительно изучают поведение людей, собирают информацию, изучают методы, которыми люди пользуются, и на основе этих данных совершают киберпреступления. Поэтому главное — не доверяйте незнакомцам и соблюдайте бдительность.

Поймите, что вы — привлекательная цель для злоумышленников, и кибератака может случиться в любое время, в любом месте, на любом устройстве. Вам поможет только ваша готовность отразить эту атаку.

1. Что такое безопасность?
2. Что такое угроза безопасности?
3. Что такое информационная безопасность?
4. В каком законодательном документе введено понятие «информационная система»?
5. Что такое кибербезопасность?
6. Что означает слово-приставка «кибер»?
7. Как произносится слово «cyber» в английском языке?
8. Почему защита информации в современном мире является сложной задачей?
9. Что такое уязвимость информационной инфраструктуры?
10. Что такое кибератака?
11. Что скрывается за аббревиатурой DDoS?
12. Что такое социальная инженерия?
13. В чем схожи фишинг и социальная инженерия?
14. Что такое обеспечение кибербезопасности?
15. Что такое киберустойчивость?
16. Почему обучение пользователей занимает особое место в системе мер обеспечения кибербезопасности?
17. К каким последствиям может привести кибератака на уровне пользователя?

Упражнения

1. Приведите примеры умышленных воздействий на информационные инфраструктуры.
2. Приведите примеры кибератак.
3. Приведите другие названия DDoS-атак.
4. Назовите возможные цели DDoS-атак.
5. Найдите в Интернете определение эксплойта.
6. Найдите в Интернете и приведите примеры видов эксплойтов.
7. Выясните в Интернете, что такое претекстинг.
8. Выясните в Интернете определение и происхождение слова «хакер».