ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 004.056

АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

© 2021 В. Д. Исичко, А. В. Линкина

Воронежский институт высоких технологий (Воронеж, Россия)

В статье рассматриваются основные понятия информационной безопасности и ее реализации при осуществлении трансформационного перехода к цифровым инструментам. Даются понятия кибербезопасности, кибертерроризма, кибератак. Описываются методы противодействия в условиях реализации национальной программы «Цифровая экономика Российской Федерации».

Ключевые слова: информационная безопасность, киберугрозы, кибербезопасность, цифровая трансформация.

Тема работы предполагает разбор основного материала по кибербезопасности и цифровой трансформации. Тесная связь этих понятий и порождает проблемы, описанные ниже.[1]

Современные технологии постоянно совершенствуются. Каждая разработка в области вычислительной техники повышает возможности пользователя по хранению, обработке информации. Любое позитивное развитие в данной области требует усовершенствование средств криптографической защиты и технического обеспечения, поэтому мероприятия кибербезопасности и цифровой трансформации необходимо выполнять параллельно.

Как известно, кибербезопасность – раздел информационной безопасности, представляющий собой процесс использования сил и средств для обеспечения конфиденциальности, целостности и доступности данных. Целью обеспечения кибербезопасности является защита информации. Для обеспечения безопасности данных могут быть применены меры, среди которых существуют: контроль доступа, обучение персонала, проверка, отчётность, оценка рисков, тестирование на проникновение и требование авторизации.

В Доктрине информационной безопасности Российской Федерации утверждённой Указом Президента Российской Федерации № 646 от 5 декабря 2016 г. представлена система официальных взглядов России на обеспечение национальной безопасности в информационной сфере. Согласно документу, в настоящее время растут масштабы компьютерной преступности в кредитно-финансовой сфере и при обработке персональных данных с использованием информационных технологий. Увеличивается количество преступлений, связанных с нарушением прав человека, в частности, в сфере неприкосновенности частной жизни, личной и семейной тайны. Остается высоким уровень зависимости российской промышленности от зарубежных технологий. Планы на создание отечественной микроэлектронной базы и программного обеспечения требуют пересмотра или, как минимум, совершенствования. Средства связи и вычислитель-

Исичко Валерия Дмитриевна – Воронежский институт высоких технологий, студент.
Линкина Анна Вячеславовна – Воронежский институт высоких технологий, ст. преп., anna_linkina@rambler.ru.

ной техники также являются слабым звеном российского производства. Всё это делает нашу страну зависимой от заграничных интересов. Одним из важнейших направлений обеспечения кибербезопасности является ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и систем обеспечения информационной безопасности. Выполнение этих целей осуществляется за счет создания, улучшения отечественных разработок.

Кибербезопасность осуществляет противодействие небольшому перечню угроз. Киберпреступления организуются с целью взломать систему, нарушить ее работу и/или получить денежные средства. Кибератаки направлены на перехват информации политического толка. Кибертерроризм направлен на хаотическое разрушение электронных систем хранения данных с целью вызвать у населения страх и посеять панику.

В условиях цифровой трансформации вероятность возникновения перечисленных угроз возрастает. В рамках национальной программы «Цифровая экономика» планируется цифровое преобразование предприятий государственного и частного сектора. Мероприятия программы направлены на поддержание нужд государственного управления и достижение достаточно крупного перечня целей. Создание новой среды возникающих отношений государства, граждан и бизнеса поможет наладить взаимодействие сторон. Повышение эффективности оказания государственных и коммерческих услуг гарантирует существенный рост спроса на данный вид деятельности. Формирование высокоскоростной системы обработки, хранения и передачи информации вместе с выполнением требований её функционирования создаст современную, устойчивую инфраструктуру и множество рабочих мест. Заполнить недостаток в кадрах поможет улучшение существующей системы обучения специалистов;

Цифровая трансформация – это трансформация системы управления путём пересмотра большого количества составляющих её элементов. Среди них стратегии, модели, операции, продукты. Переход обеспечивается принятием цифровых технологий. Трансформация призвана ускорить экономический рост коммерческих и увеличить эффективность деятельности некоммерческих организаций. В наши дни организации используют большие объемы личных данных, которые создаются для повышения качества обслуживания заказчиков в социальных сетях, мессенджерах и мобильных приложениях. Компании, которые переходят на цифровые технологии, используют этот массив персонализированных данных, чтобы улучшить свою продукцию и услуги. Термин «цифровая трансформация» на данный момент не имеет чёткого определения, а с годами оно получает всё больше толкований

Цифровая трансформация может привести экономику к стадии цифровой зрелости, влияя как на отдельные предприятия, так и на все сферы жизни общества. Решения в этой области мотивируют формирование новых видов деятельности и творческого развития. Цифровая трансформация является основным противоречием. Планируя проведение цифровых преобразований, начальники организаций обязаны учитывать изменения, с которыми сталкиваются их сотрудники, поскольку работники только приспосабливаются к незнакомым технологиям.

Важным фактором цифровой трансформации является ее темп. Именно он определяет трудности в обеспечении кибербезопасности. Требования по обеспечению информационной безопасности всегда направлены на достижение следующих аспектов компьютерной безопасности.

Конфиденциальность – это взаимосвязь между сбором и распространением данных, технологиями, ожиданиями общественности в отношении конфиденциальности и связанными с ними правовыми и политическими проблемами. Засекреченная информация должна быть доступна только тому, кому она предназначена. Такую информацию невозможно получить, прочитать, изменить, передать, если на это нет соответствующих прав доступа. Также Федеральный закон «Об информации, информационных технологиях и о защите информации» гласит о том, что конфиденциальность информации – требование не передавать информацию третьим лицам без согласия ее обладателя, обязательное для выполнения лицом, получившим доступ к этим данным. Чтобы обеспечить конфиденциальность информации, её нужно закрыть, скрыть, зашифровать или раздробить. В условиях цифрового преобразования выполнение этих мероприятий не

только существенно упрощает пользователю его задачу, но и одновременно делает информацию более уязвимой. При наличии соответствующего оборудования потенциальному злоумышленнику становится гораздо проще получить доступ к интересующим его данным. Существующие системы защиты информации должны постоянно обновляться и быть в готовности к любым атакам.

Целостность – это, зачастую, актуальность информации и отсутствие противоречий, защищенность данных от разрушения и несанкционированного изменения. Информация, на основе которой принимаются решения, должна быть достоверной, защищенной от различных искажений и точной. Целостность – это отсутствие неправомерных искажений, различных вкраплений или удаления информации. Гарантия целостности особо важна тогда, когда данные представляют большую ценность. При цифровой трансформации становится удобнее хранить большие объемы информации на электронных носителях. С каждым годом потенциальный объем памяти в создаваемых накопителях растет, ведь прогресс не стоит на месте. Однако, при взаимодействии баз данных с открытыми сетями упрощается задача злоумышленника. Толковому специалисту проще получить доступ к информации при помощи компьютера, чем взламывать сейф за семью печатями. От изменения и уничтожения данные защищают резервным копированием и методами, обеспечивающими конфиденциальность, а отсутствие искажений проверяют с помощью хеширования.

Доступность – возможность в относительно короткие сроки получить требуемую услугу. Информация, сервисы и соответствующие службы, средства взаимодействия и связи должны быть доступны и готовы к работе всегда, когда в них возникает необходимость. Доступность – это обеспечение своевременного и надежного доступа к информации и информационным сервисам. В эпоху цифровых преобразований требования к доступности информации возросли. Информатизация потребителей ускорила свои темпы, но появился и ряд проблем. Частыми случаями нарушения доступности являются сбои в электропитании и работе программных и/или аппаратных средств. От первых систему защищают установкой резервных источников электропитания, от других неполадок - устранением причин их вызывающих. Также имеет место и распределенная DDoS-атака, провоцирующая отказ в обслуживании. С подобными атаками борются отсечением паразитного трафика.

Таким образом, цифровая трансформация наряду с решением многих проблем и совершенствованием управления и взаимодействия в предприятиях государственного и частого сектора имеет и ряд недостатков. Негативное влияние снижается путем формирования надежной системы охраны средств сбора, хранения и обработки информации и созданием комфортной среды для качественного обучения специалистов в этой области.

ЛИТЕРАТУРА

1. Анисимов А. А. Менеджмент в сфере информационной безопасности: учебное пособие / Анисимов А. А. – Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 211 с. – ISBN 978-5-4497-0328-6. – Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. – URL: https://www.iprbookshop.ru/89443.html (дата обращения: 16.11.2021). – Режим доступа: для авторизир. пользователей.

2. Бабуханян А. Б. Информационная и кибербезопасность в условиях цифровизации государственного управления / Бабуханян А. Б. // Научные труды северо-западного института управления РАНХИГС. – 2018. – № 4 (36). – С. 39 – 43.

3. Белоус А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / Белоус А. И., Солодуха В. А. – М.: Вологда: Инфра-Инженерия, 2020. – 692 с. – ISBN 978-5-9729-0486-0. – Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. – URL: https://www.iprbookshop.ru/98349.html (дата обращения: 16.11.2021). – Режим доступа: для авторизир. пользователей.

4. Белоус А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / Белоус А. И., Солодуха В. А. – Москва: Техносфера, 2021. – 482 с.

5. Дождиков В. Г. Краткий энциклопедический словарь по информационной безопасности / Дождиков В. Г., Салтан М. И. – Москва: Энергия, 2010. – 239 с. – ISBN 978-

5-98420-043-1. – Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. – URL: https://www.iprbookshop.ru/5729.html (дата обращения: 16.12.2021). – Режим доступа: для авторизир. пользователей.

6. Сологубова Г. С. Составляющие цифровой трансформации: монография / Г. С. Сологубова. – М.: Издательство Юрайт, 2021. – 147 с.

7. Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин – Саратов: Профобразование, 2019. – 702 с.

DIGITAL TRANSFORMATION IN THE COMPUTER GAMES INDUSTRY

© 2021 V. D. Isichko, a. V. Linkina

Voronezh institute of High Technologies (Voronezh, Russia)

The article discusses the basic concepts of information security and its implementation in the implementation of the transformational transition to digital tools. The concepts of cyber security, cyber terrorism, cyber attacks are given. Methods of counteraction in the context of the implementation of the national program "Digital Economy of the Russian Federation" are described.

Keywords: information security, cyber threats, cyber security, digital transformation.