Образование как важнейший фактор кибербезопасности.

Пономарева М.Г.,

ГК «Аудиторы корпоративной безопасности», Москва, Россия,

ponomareva@ruakb.ru

В статье рассматривается вопрос обеспечения кибербезопасности и обучения киберграмотности детей, начиная с младшего возраста. Приведены основные проблемы кибербезопасности в международных масштабах, проведен краткий анализ факторов, влияющих на позицию специалистов информационной безопасности в противостоянии с представителями теневых информационных сетей. Произведен анализ модели угроз использования персональных цифровых устройств с учетом детской специфики, как наиболее опасный показан человеческий фактор.

Ключевые слова: дети, кибербезопасность, образование, киберграмотность, человеческий фактор.

Пономарева Мария Геннадьевна, руководитель отдела, ГК «Аудиторы корпоративной безопасности», Москва, Россия

В данной работе затрагивается образование, как важнейший фактор, обеспечивающий кибербезопасность каждого человека, использующего цифровые устройства. В 2018 году был дан старт ежегодному международному конгрессу профессионалов информационной безопасности, проводимому под эгидой Сбербанка, International Cyber Congress (ICC). Кибербезопасность – относительно новый термин, обозначающий как информационную безопасность предприятий, так и цифровую безопасность персональных пользовательских устройств, таких, как смартфоны, планшеты, системы «умный дом» и прочие подобные системы.

Проблемы обеспечения кибербезопасности являются международными и межгосударственными, что подтверждает регулярное участие в упомянутом

конгрессе представителей правительственных и международных исполнительных организаций. Государственный приоритет решения проблемы отражает и то, что в 2018 году участников первого конгресса личным присутствием отметил президент Российской Федерации В.В. Путин. В работе конгресса также принимали участие глава Сбербанка Г.О. Греф, высшее руководство банка ВТБ, Ассоциация Банков России, FinCert, VISA, SWIFT, Интерпол, МИД, МВД, RT, а также лидеры цифровой индустрии, среди которых отметились «Лаборатория Касперского», InfoWatch, Microsoft, Cisco, HUAWEI, IBM Security, Ростелеком.

Глобально можно выделить следующие вопросы, требующие решения:

1. В эпоху цифровизации государство становится носителем цифрового образа страны;
2. Количество кибератак растет вместе с расходами компаний на безопасность;
3. Наибольшие киберугрозы в финансовой отрасли экономики;
4. Данные – один из самых ценных активов;
5. Любая отрасль может стать объектов кибератаки;
6. Ограничения и блокировки ведут к росту уязвимости.

По данным прошедших конгрессов [3], впечатляют прогнозы потерь от кибератак – до $8 трлн. к 2022 году. Пугающим выглядит прогноз дефицита специалистов информационной безопасности – к 2022-му году он может достигнуть 1,8 млн. человек. В сфере деятельности предприятий частично эту проблему поможет решить использование искусственного интеллекта. Массовое повышение киберграмотности обычных пользователей цифровых устройств поможет предотвратить последствия многих видов атак злоумышленников.

Успешное противостояние специалистов защиты информации представителям теневых информационных сетей осложняется следующими основными моментами:

1. Кибергруппировки злоумышленников интернациональны;
2. Распределены по всему миру;
3. Киберпреступления это бизнес;
4. Нет никаких сдерживающих причин.

Атаки на программное и аппаратное обеспечение безопасности «наиболее часто используются злоумышленниками. Связано это с тем, что для их реализации нет необходимости обладать обширными познаниями в области математики. Достаточно быть квалифицированным программистом» или психологом. [1]

Наиболее слабым звеном в построении любой системы защиты является человеческий фактор. Пренебрежение к вопросам собственной безопасности, умышленные действия по нарушению конфиденциальности данных, пользовательские ошибки – вот главные обстоятельства, влияющие на использование цифровых устройств в личных целях и в работе организаций. «Чем более совершенными становятся программные и аппаратные методы защиты информации, тем более весомую роль играют атаки на человеческий фактор – использование злоумышленниками обычных человеческих слабостей специалистов, имеющих доступ к конфиденциальной информации, методик социальной инженерии.» [3]

Практика работы с пользователями при внедрении различных проектов систем информационной безопасности показывает, что люди элементарно не понимают риски, связанные с использованием персональных цифровых устройств. Вследствие этого можно утверждать, что киберграмотность является необходимым первым уровнем защиты. В модели угроз информации каждого пользователя можно выделить наиболее значимые:

1. Цифровые следы не стираются;
2. Люди не понимают риск от кражи цифровых следов;
3. Доступ к цифровому образу – огромная угроза (включая манипулирование, шантаж, кражу денег и др.);

4. К 2020-му году предполагается в среднем по 3 устройства на человека, подлежащих защите;
5. Каждое подключение – потенциальная точка доступа к цифровому образу.

Киберграмотность в эпоху информационных войн имеет жизненно важное значение и для взрослых пользователей, и для детей. Говоря о подрастающих поколениях, необходимо выделить специфические особенности в их повседневном обращении с персональными цифровыми устройствами:

1. Дети с раннего детства привыкли использовать цифровые устройства для развлечения и учебы, видят в них естественное «продолжение себя»;
2. Возникает беспечность, дети не видят никакой угрозы в том, что представляет для них абсолютно обычные действия;
3. Дети не представляют истинного масштаба угроз и появляется иллюзия безопасности в силу использования некоторых систем защиты информации;
4. Юношеский максимализм, особенно в подростковом возрасте, требует новых способов самовыражения, советы взрослых воспринимаются агрессивно как попытки излишнего контроля;
5. Талантливые дети имеют подсознательную жажду признания и при некоторых условиях могут вступить в ряды киберпреступников со всеми последствиями;
6. Социальная инженерия – дети легко могут стать добычей злоумышленников вплоть до смертельных случаев;
7. Привычка сохранять данные на любимом устройстве является серьезной угрозой для защиты интеллектуальной собственности, включая кражу или утерю собственных проектов талантливых детей.

В вопросе поддержки талантливых детей необходимо уделять внимание всем перечисленным обстоятельствам. Отсутствие наставников в сфере кибербезопасности и взаимопонимания поколений «отцов и детей» в эпоху информационных войн может привести к глобальным мировым проблемам.

«У большинства людей – независимо от того, на чем основаны их системы ценностей, - есть набор представлений о подобающем поведении и профессиональной добросовестности, причем эти представления обладают созидательным потенциалом в масштабах организации» [2] и всего мира.

Решение вопроса видится через осуществление параллельной работы в двух взаимосвязанных сферах:

1. Обучение специалистов по кибербезопасности;
2. Повышение киберграмотности пользователей всех возрастных категорий.

В заключение можно отметить, что именно комплексный подход, включающий образовательные программы и развитие технических средств защиты информации, способен надлежащим образом обеспечить должную защиту конфиденциальных данных пользователей и организаций.

Финансирование

Работа выполнена в процессе проведения учебной практики со студентами колледжа телекоммуникаций в качестве внештатного преподавателя.

Благодарности

Автор благодарит за помощь в анализе материалов научного руководителя проекта Янкевского А.В.

Литература

1. *Росляков А.В.* Виртуальные частные сети. Основы построения и применения. – М.: Эко-Трендз, 2006. – 304 с.: ил.

2. *Кристенсен Ральф.* Стратегическое управление человеческими ресурсами: дорожная карта. От великой идеи к деловой практике/[Пер. с англ. А.Столярова]. – М.: ЗАО «Олимп-Бизнес», 2011. – 288 с: ил.
3. *Пономарева М.Г.* Влияние человеческого фактора на обеспечение информационной безопасности в развитии сферы медицинских услуг. // Развитие инновационной экономики в России. Сборник материалов 4-й Всероссийской заочной научно-практической конференции. Научные труды Вольного экономического общества. Том 174, 2013. - 442 с. // С. 396 – 401.
4. Материалы Международного КиберКонгресса ICC [Электронный ресурс] // URL: https://icc.moscow/ru/ (дата обращения: 19.11.2019);

The education as an essential factor in cybersecurity

Ponomareva M.G.,

GC «Auditors of corporate security», Moscow, Russia

ponomareva@ruakb.ru

The article considers the issue of ensuring cybersecurity and teaching cyber literacy of children, starting from a young age. The main problems of cybersecurity on an international scale are presented, a brief analysis of the factors affecting the position of information security specialists in the confrontation with representatives of shadow information networks is carried out. The analysis of the threat model for the use of personal digital devices, taking into account the specifics of children, as the most dangerous human factor is shown.

Keywords: children, cybersecurity, education, cyber literacy, human factor

Funding

The work was carried out in the process of conducting educational practice with students of the College of Telecommunications as a freelance teacher.

Acknowledgements

The author is grateful for assistance in data analysis Yankevsky A.V.

Ponomareva Mariya Genndievna, head of sales department, GC «Auditors of corporate security», Moscow, Russia

References

1. *Roslyakov A.V.* Virtual'nye chastnye seti. Osnovy postroyeniya i primeneniya. – M.: Eko-Trandz, 2006. – 304 s.: il.
2. *Kristensen Ralf.* Strategicheskoye upravleniye chelovecheskimi resursami: dorozhnaya karta. Ot velikoy idei k delovoy praktike/ [Per. s angl. A.Stolyarova]. – M.: ZAO «Olimp-Biznes», 2011. – 288 s: il.
3. *Ponomareva M.G.* Vliyanie chelovecheskogo faktora na obespecheniye informatsionnoy bezopasnosti v razvitii sfery meditsinskih uslug. // Razvitie innovatsionnoy ekonomiki v Rossii. Sbornik materialov 4-i Vserossiyskoy zaochnoy nauchno-prakticheskoy konferentsii. Nauchnye Trudy Vol'nogo ekonomicheskogo obschestva. Tom 174, 2013.. - 442 s. // S. 396 – 401.
4. Materialy Mezhdunarodnogo KiberKongressa ICC [Elekrtonnyi resurs] // URL: https://icc.moscow/ru/ (Accessed: 19.11.2019);