CYBER SECURITY UZ

КИБЕРБЕЗОПАСНОСТЬ РЕСПУБЛИКИ УЗБЕКИСТАН

ИТОГИ 2020 ГОДА

Содержание

Введение

Узбекистан уверенно вошел в век цифровизации, о чем свидетельствуют поэтапные действия правительства направленные на увеличение скорости и качества Интернета, повсеместного внедрения информационно-коммуникационных технологий во все сферы жизнедеятельности страны.

При этом, особое внимание уделяется вопросам обеспечения кибербезопасности, о чем свидетельствуют осуществляемые работы государственного унитарного предприятия «Центр кибербезопасности», на который возложен ряд задач по обеспечению защиты от потенциальных кибератак, бесперебойного функционирования объектов информатизации и критической информационной инфраструктуры Республики Узбекистан.

В целях качественного и своевременного выполнения возложенных задач, Центром кибербезопасности проводится мониторинг событий, предотвращение и реагирование на угрозы и инциденты кибербезопасности в национальном сегменте сети Интернет. В представленном отчёте приводится основная статистика по угрозам и инцидентам кибербезопасности в 2020 году и информация о принятых мерах по обеспечению кибербезопасности.

Угрозы

В течении 2020 года выявлено более 27 000 000 событий вредоносной и подозрительной сетевой активности, исходящей из адресного пространства национального сегмента сети Интернет, которые в свою очередь представляли угрозы безопасному и стабильному функционированию информационных систем и ресурсов государственных органов и иных организаций (Рис. 1), в частности:

Рис. 1. Основные виды выявленных угроз.

Ниже приведена динамика вышеописанных событий кибербезопасности, в разрезе ведущих операторов сетей телекоммуникаций республики (Рис. 2).

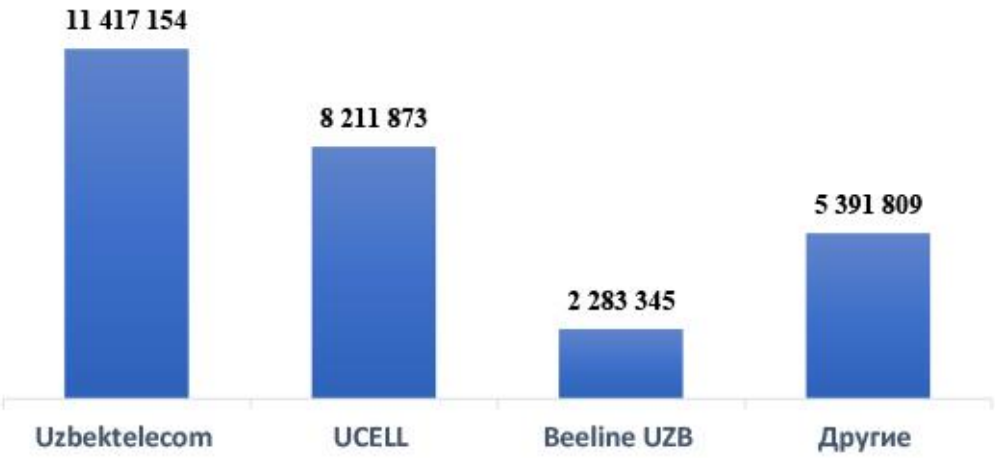

Рис. 2. События кибербезопасности в разрезе операторов связи.

По итогам 2020 года из 86 679 зарегистрированных доменов, активными являются порядка 30 000 доменов. Из них, более 12 500 доменов имеют SSL-сертификат безопасности и у порядка 300 доменов сертификат просрочен (Рис. 3). Ниже приведена соответствующая статистика.

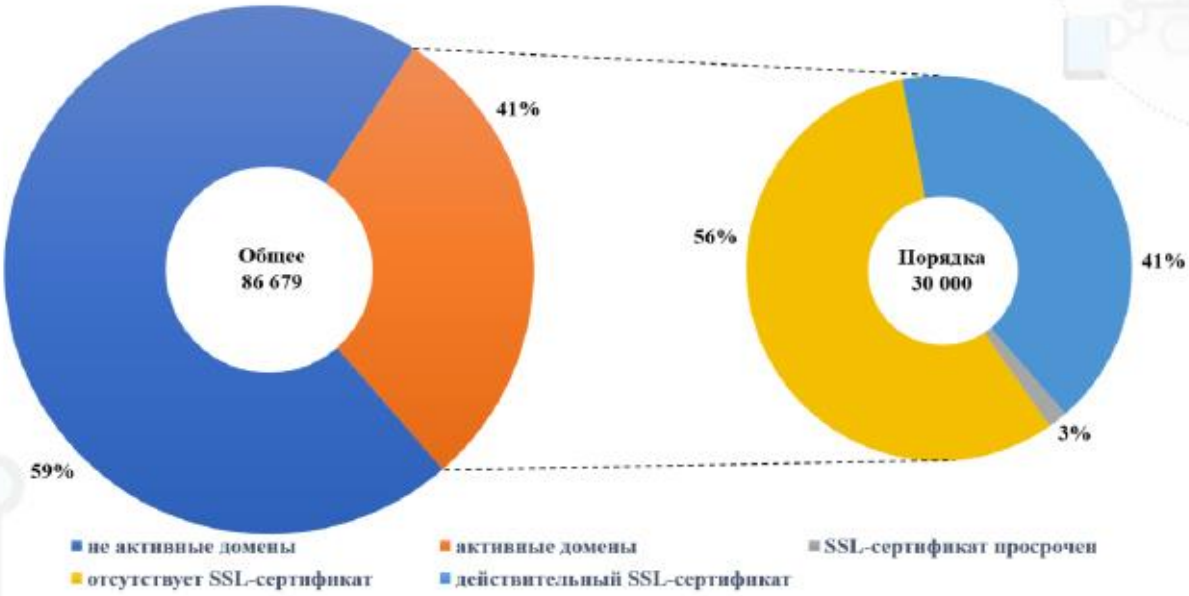

Рис. 3. Информация о доменах и наличии сертификата безопасности.

Инциденты и события

В рамках безопасного функционирования информационных систем и веб-сайтов, за прошедший 2020 год выявлено 680 событий безопасности (Рис. 4), в том числе технические неполадки, что составляет порядка 1 000 000 минут недоступности (простоя) веб-сайтов.

Рис. 4. Основные виды выявленных событий.

В ходе мониторинга информационных систем, подключенных к межведомственной сети передачи данных (МСПД), зафиксировано 9 955 152 событий безопасности (Рис. 5), из которых 94 147 событий могли привести к несанкционированному получению доступа и утечке конфиденциальной информации (Рис. 6).

Рис. 5. Выявленные события в информационных системах, подключенных к межведомственной сети передачи данных.

Рис. 6. Критические события.

По итогам мониторинга инцидентов кибербезопасности, совершенных в отношении веб-сайтов доменной зоны «UZ», зафиксировано 342 инцидента, из которых наибольшее количество приходится на несанкционированную загрузку контента (НЗК) – 306, остальные связаны с несанкционированным изменением главной страницы (Deface) – 36.

Анализ мониторинга показал, что веб-сайты государственного сектора (81 инцидент) подвержены атакам в 3 раза реже, по сравнению с частным сектором (261 инцидент).

По сравнению с 2019 годом, наблюдается динамика роста количества инцидентов, связанных с несанкционированной загрузкой веб-контента и уменьшение количества инцидентов, связанных с изменением главной страницы (Рис. 7).

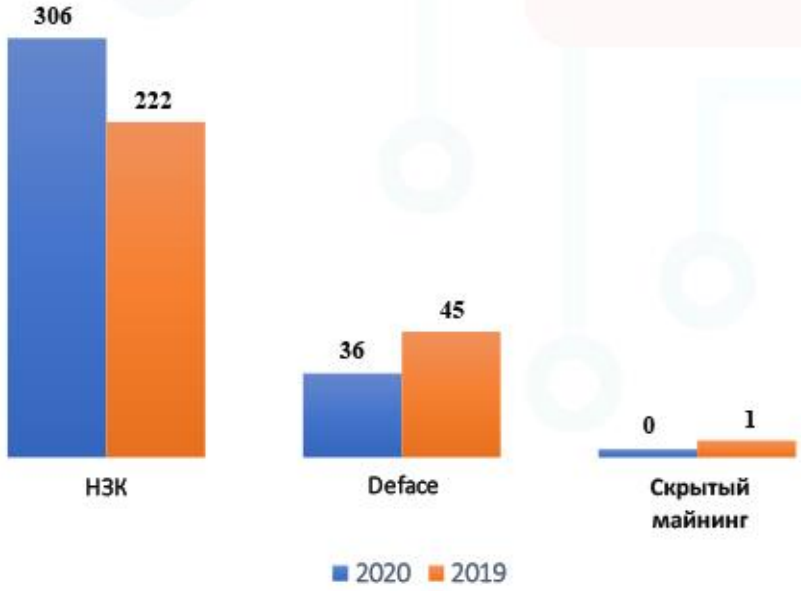

Рис. 7. Инциденты кибербезопасности за 2020 и 2019 года.

Детальный анализ инцидентов показал, что наиболее уязвимыми (часто атакуемыми) являются веб-сайты разработанные на системах управления контентом «Wordpress», «Joomla», «Open Journal Systems» и «Drupal» (Рис. 8).

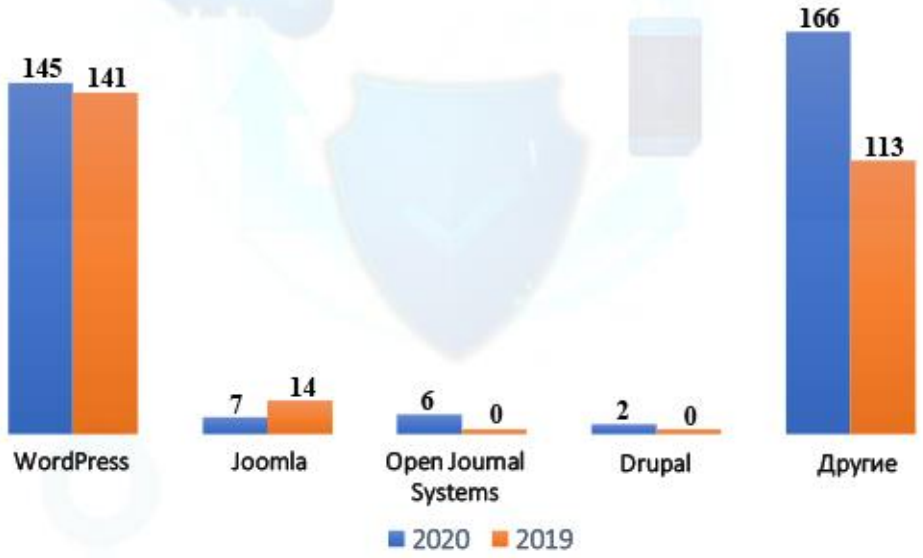

Рис. 8. Сравнение инцидентов 2020 и 2019 года.

Расследование инцидентов кибербезопасности

В рамках выявления вредоносного контента и анализа его причастности к правонарушениям в информационном пространстве проведены расследования инцидентов кибербезопасности, в ходе которых установлены причины и способы их осуществления (Рис. 9).

Основными причинами и способами успешной реализации хакерских атак являются: перебор паролей к учётным записям (Brute force), устаревшая или уязвимая версия системы управления контентом (CMS), SQL-инъекции, устаревшие плагины (Рис. 9).

В частности, по итогам расследований выявлено более 2690 вредоносных файлов, а также источники (страны), из которых проводились несанкционированные действия, деструктивного характера: Румыния, Германия, Египет, Республика Словакия, США, Индонезия, Китай, Российская Федерация, Великобритания, Франция, Саудовская Аравия, Тунис, Украина, Нидерланды, Южная Корея, Канада, Франция, Турция, Польша, Вьетнам, Индия.

По сравнению с аналогичным периодом 2019 года наблюдается динамика роста количества инцидентов, совершенных в отношении веб-сайтов государственных и хозяйственных органов на 144%.

Рис. 9. Причины и способы возникновения инцидентов.

Уязвимости

В ходе выполнения мероприятий по повышению уровня защищенности информационных систем и ресурсов доменной зоны «UZ» за отчётный период проведено 297 изучений и экспертиз.

По итогам проведенных работ выявлено 695 уязвимостей кибербезопасности (Рис. 10), о наличии которых своевременно были оповещены владельцы информационных систем и ресурсов. Ниже приведена информация о выявленных уязвимостях:

- высокого уровня критичности – 466;
- среднего уровня критичности – 205;
- низкого уровня критичности – 24.

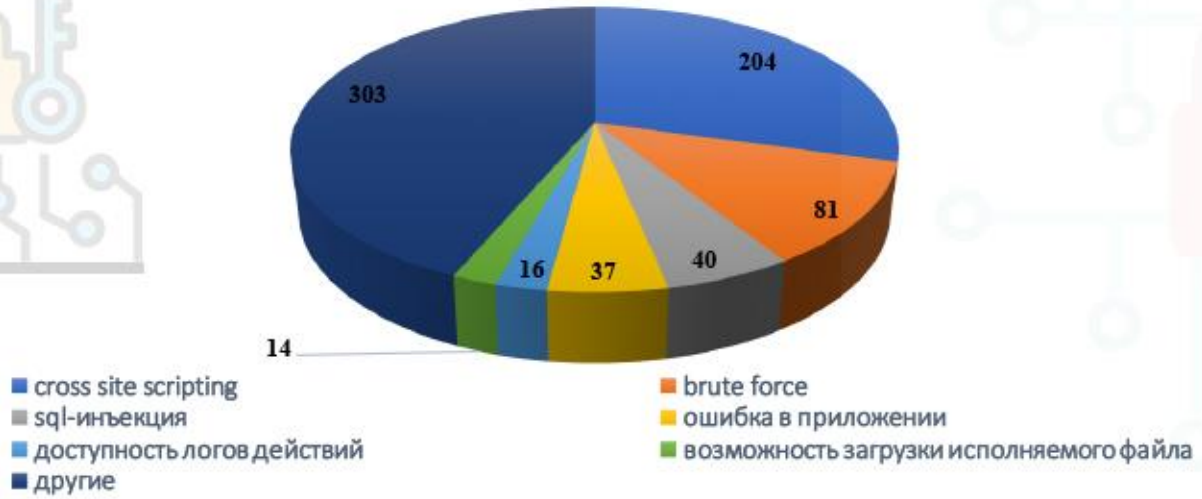

Рис. 10. Основные виды выявленных уязвимостей.

Эксплуатация злоумышленниками, вышеописанных уязвимостей могла привести к утечке персональных данных граждан Республики Узбекистан.

Сертификация

В целях подтверждения качества систем управления информационной безопасности, аппаратных средств, программных продуктов, информационно-коммуникационных технологий, телекоммуникационного оборудования и иных технических средств, в том числе средств защиты информации, Центром проводится сертификация на соответствие продукта требованиям нормативных документов по информационной и кибербезопасности.

За 2020 год, сертификаты соответствия успешно получили 45 программных обеспечений (Рис. 11), в числе которых имеется и операционная система общего назначения «Cent OS Linux 8» версия 5.8.14.

Рис. 11. Сертифицированное программное обеспечение.

CYBER SECURITY UZ

Центр кибербезопасности

info@csec.uz www.csec.uz (55) 502-10-10